华图网校
SINCE 2001
V.HUATU.COM
乐享品质　高效学习

专业课

计算机

信息安全

袁礼

华图网校

目录

（一）信息安全问题 1
（二）信息系统中的主要安全问题 1
（三）网络与信息安全的主要任务 1
（四）我国信息安全的现状 2
（五）信息安全威胁 3
（六）常见安全威胁 4
（七）安全威胁分类 5
（八）信源、信宿、信息之间的关系 5
（九）信息安全的基本要素 6
（十）信息安全的目的 6
（十一）信息安全保护技术 6
（一）信息安全研究内容及相互关系 7
（二）信息安全理论研究 7
（三）信息安全应用研究 8
（一）安全标准研究 10
（二）OSI 信息安全体系结构 11
（三）信息安全发展阶段 12

信息安全

本章内容：

- 信息安全的目标
- 信息安全的研究内容
- 信息安全的发展

一、信息安全的目标

（一）信息安全问题

信息

信息就是消息，是关于客观事实的可通讯的知识。信息可以被交流、存储和使用。

信息安全

国际标准化组织(ISO)的定义为：“为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露”。

（二）信息系统中的主要安全问题

1、网络可靠性问题（备份,网络管理，计费等)

2、系统本身的缺陷（芯片、操作系统,数据库后门等)

3、恶意攻击和破坏（黑客攻击,病毒破坏等)

4、信息安全问题（信息窃取,假冒,抵赖等)

（三）网络与信息安全的主要任务

（1）网络安全的任务：

保障各种网络资源稳定可靠的运行，受控合法的使用。

（2）信息安全的任务：

保证：机密性、完整性、不可否认性、可用性

（3）其他方面：

病毒防治，预防内部犯罪

（四）我国信息安全的现状

1、信息与网络安全的防护能力较弱。

- 用不加锁的储柜存放资金（网络缺乏安全防护）；
- 让“公共汽车”运送钞票（网络缺乏安全保障）；
- 使用“邮寄”传送资金（转账支付缺乏安全渠道）；
- 用“商店柜台”存取资金（授权缺乏安全措施）；
- 拿“平信”邮寄机密信息（敏感信息缺乏保密措施）等。

2、基础信息产业相对薄弱，核心技术严重依赖国外。对引进的信息技术和设备缺乏保护信息安全的有效管理和技术改造。

- 硬件方面：电脑制造业有很大的进步，但许多核心部件都是原始设备制造商的，关键部位完全处于受制于人的地位。
- 软件方面：面临市场垄断和价格歧视的威胁。美国微软几乎垄断了我国电脑软件的基础和核心市场。
- 我国从发达国家和跨国公司引进和购买了大量的信息技术和设备。在这些关键设备有一部分可能隐藏着“特洛伊木马”，对我国政治、经济、军事等的安全存在着巨大的潜在威胁。

3、信息安全管理力度还要加强,法律法规滞后现象急待解决。

- 信息安全特别是在经济等领域的安全管理条块分割、相互隔离，缺乏沟通和协调。没有国家级的信息安全最高权威机构以及与国家信息化进程相一致的信息安全工程规划。

4、信息犯罪在我国有快速发展的趋势。

- 西方一些国家采取各种手段特别是电子信息手段来窃取我国的各类机密，包括核心机密。此外，随着信息设备特别是互联网的大幅普及，各类信息犯罪活动亦呈现出快速发展之势。

5、具有知识产权的信息与网络安全产品相对缺乏,且安全功能急待提高。

- 近年来，信息网络安全技术和产品的研究、开发、应用发展迅速，其中病毒防治等一些关键性产品实现了国产化。但是“这些产品安全技术的完善性、规范性、实用性还存在许多不足，特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面存在很大距离，理论基础和自主技术手段也需要发展和强化”。

6、全社会信息安全意识急待提高，加强专门安全人才的培养。

（五）信息安全威胁

信息安全威胁：指某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用性等等所造成的危险。

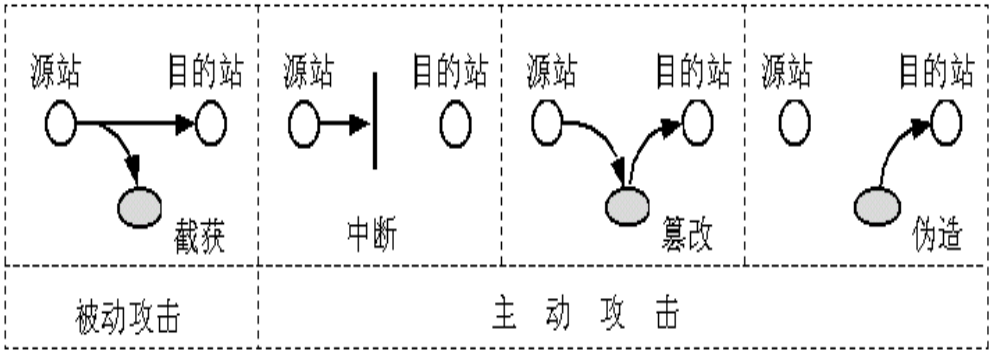
攻击就是对安全威胁的具体体现。虽然人为因素和非人为因素都可以对通信安全构成威胁，但是精心设计的人为攻击威胁最大。

(1)截获(interception)

(2)中断(interruption)

(3)篡改(modification)

(4)伪造(fabrication)



被动攻击：

目的是窃听、监视、存储数据，但是不修改数据。很难被检测出来，通常采用预防手段来防止被动攻击，如数据加密。

主动攻击：

修改数据流或创建一些虚假数据流。常采用数据加密技术和适当的身份鉴别技术。

截获

以保密性作为攻击目标，表现为非授权用户通过某种手段获得对系统资源的访问，如搭线窃听、非法拷贝等

中断

以可用性作为攻击目标，表现为毁坏系统资源，切断通信线路等

篡改

以完整性作为攻击目标，非授权用户通过某种手段获得系统资源后，还对文件进行窜改，然后再把篡改过的文件发送给用户。

伪造

以完整性作为攻击目标，非授权用户将一些伪造的、虚假的数据插入到正常系统中

（六）常见安全威胁

1. 信息泄露：信息被泄露或透露给某个非授权的实体。
2. 破坏完整性：数据被非授权地进行增删、修改或破坏而受到损失。
3. 拒绝服务：对信息或其它资源的合法访问被无条件地阻止。
4. 非法使用：某一资源被某个非授权的人，或以非授权的方式使用。
5. 窃听：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。
6. 业务流分析：通过对系统进行长期监听来分析对通信频度、信息流向等发现有价值的信息和规律。
7. 假冒：通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒攻击。
8. 旁路控制：攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。
9. 授权侵犯：被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其它非授权的目的，也称作“内部攻击”。
10. 特洛伊木马：软件中含有一个察觉不出的或者无害的程序段，当它被执行时，会破坏用户的安全。这种应用程序称为特洛伊木马。
11. 陷阱门：在某个系统或某个部件中设置的“机关”，使得当提供特定的输入数据时，允许违反安全策略。
12. 抵赖：这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。
13. 重放：所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。
14. 计算机病毒：是一种在计算机系统运行过程中能够实现传染和侵害的功能程序。
15. 人员不慎：一个授权的人为了钱或利益，或由于粗心，将信息泄露给一个非授权的人。
16. 媒体废弃：信息被从废弃的磁的或打印过的存储介质中获得。
17. 物理侵入：侵入者通过绕过物理控制而获得对系统的访问；
18. 窃取：重要的安全物品，如令牌或身份卡被盗；
19. 业务欺骗：某一伪系统或系统部件欺骗合法的用户或系统自愿地放弃敏感信息。

（七）安全威胁分类

物理环境：自然灾害 ,电源故障、设备被盗

通信链路：安装窃听装置或对通信链路进行干扰

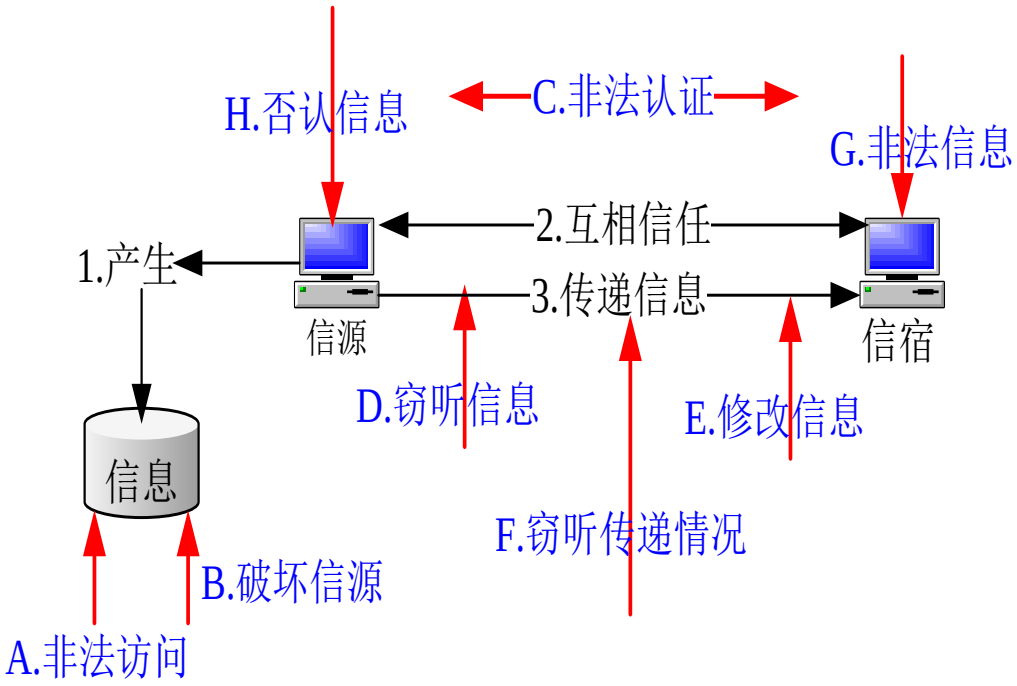
网络系统：互联网的开放性、国际性

操作系统：系统软件或硬件芯片中的植入威胁

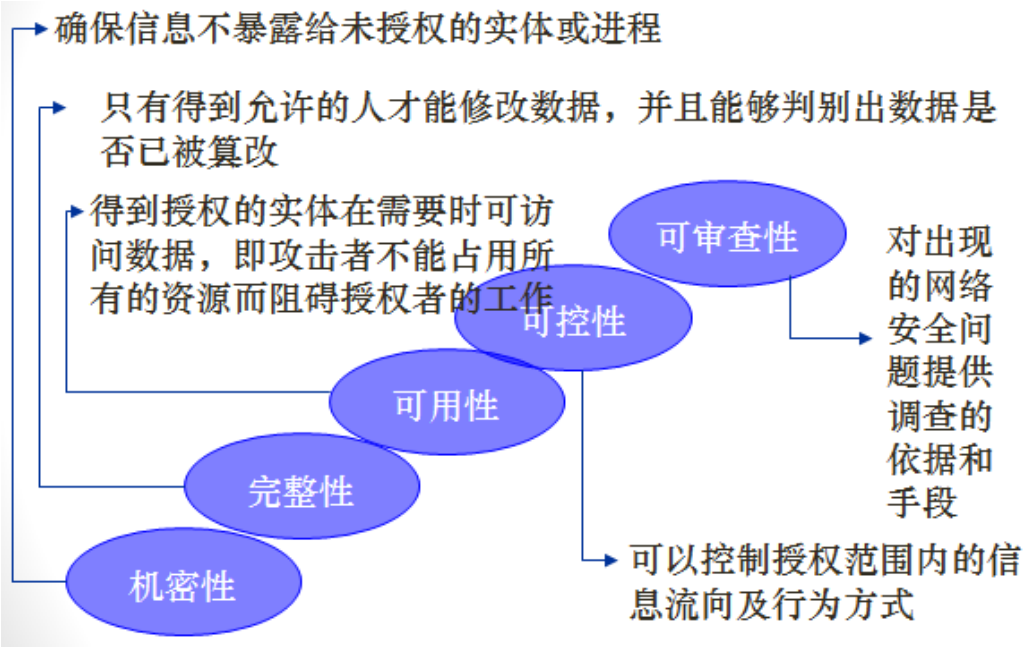
应用系统：木马、陷阱门、逻辑炸弹

管理系统：管理上杜绝安全漏洞

（八）信源、信宿、信息之间的关系



（九）信息安全的基本要素



（十）信息安全的目的

使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

使用授权机制，实现对用户的权限控制，即不该拿走 的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

使用加密机制，确保信息不暴漏给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

（十一）信息安全保护技术

（1）主动防御保护技术

数据加密、身份鉴别、存取控制、权限设置、

虚拟专用网(VPN)技术。

（2）被动防御保护技术

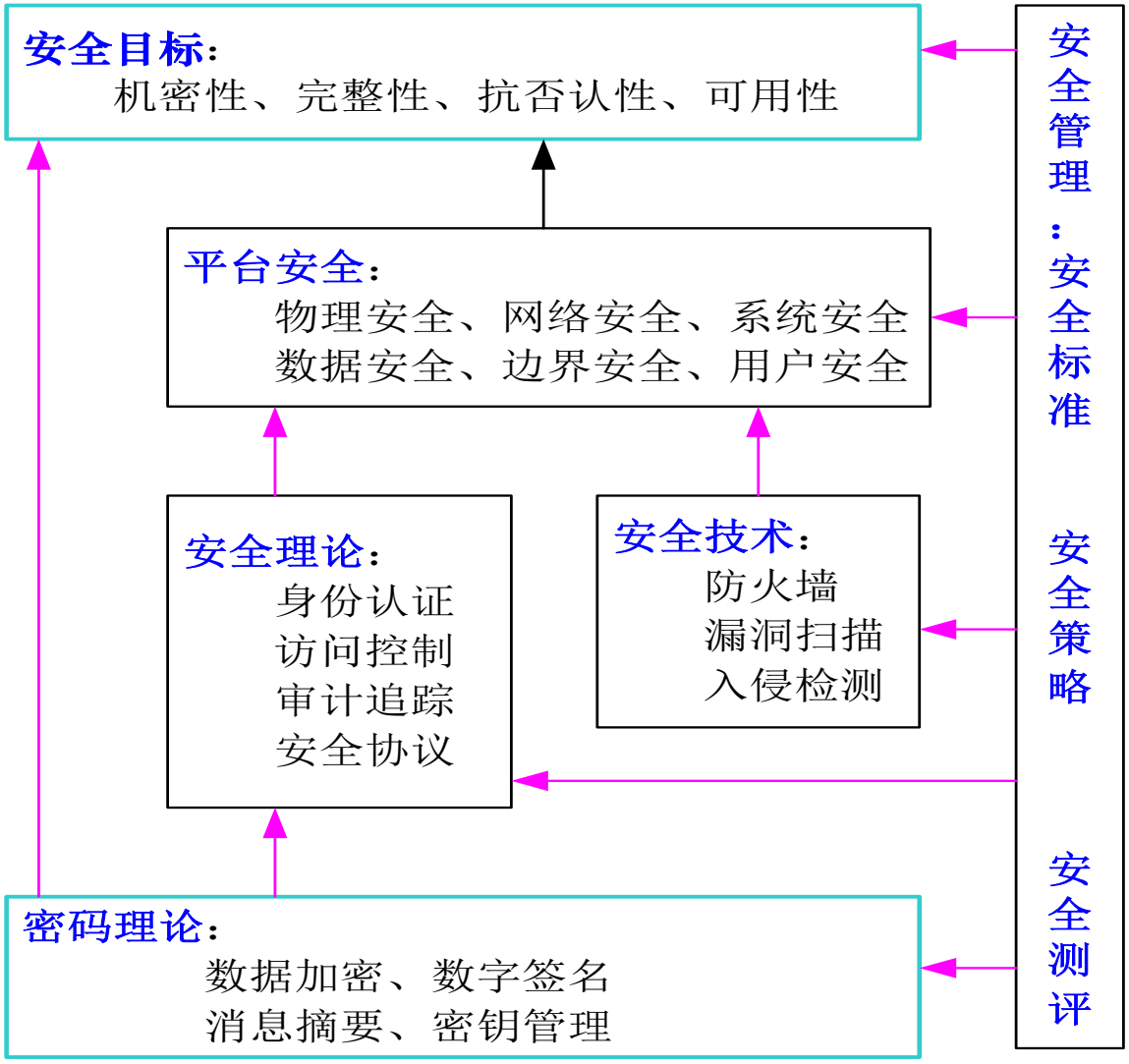
防火墙、入侵检测系统、安全扫描器、口令验证、 审计跟踪、物理保护与安全管理。

二、信息安全的目标

信息安全是一门涉及计算机科学、网络技术、通信技术、
密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

信息安全研究的内容包括
一、信息安全理论研究
二、信息安全应用研究
三、信息安全管理研究

（一）信息安全研究内容及相互关系



（二）信息安全理论研究

1、密码理论

加密：将信息从易于理解的明文加密为不易理解的密文

消息摘要：将不定长度的信息变换为固定长度的摘要

数字签名：实际为加密和消息摘要的组合应用

密钥管理：研究密钥的产生、发放、存储、更换、销毁

2、安全理论

身份认证：验证用户身份是否与其所声称的身份一致

授权与访问控制：将用户的访问行为控制在授权范围内

审计跟踪：记录、分析和审查用户行为，追查用户行踪

安全协议：构建安全平台使用的与安全防护有关的协议

（三）信息安全应用研究

1、安全技术

防火墙技术：控制两个安全策略不同的域之间的互访行为

漏洞扫描技术：对安全隐患的扫描检查、修补加固

入侵监测技术：提取和分析网络信息流，发现非正常访问

病毒防护技术：

2、平台安全

物理安全：主要防止物理通路的损坏、窃听、干扰等。

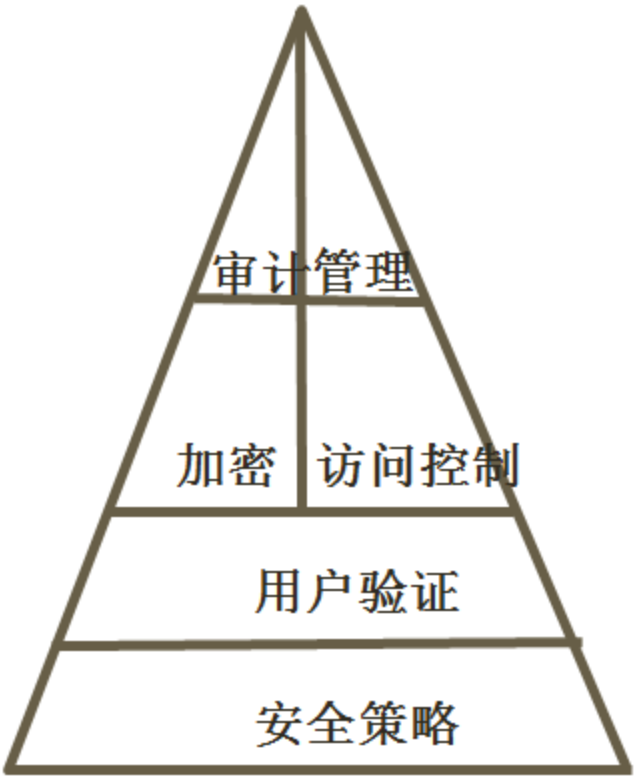
网络安全：保证网络只给授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听。

系统安全：保证客户资料、操作系统访问控制的安全，同时能对该操作系统上的应用进行审计。

数据安全：对安全环境下的数据需要进行加密。

用户安全：对用户身份的安全性进行识别。

边界安全：保障不同区域边界连接的安全性。



一、安全策略

指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的三个重要组成部分，即威严的法律、先进的技术、严格的管理。

安全策略是建立安全系统的第一道防线

给予资源合理的保护

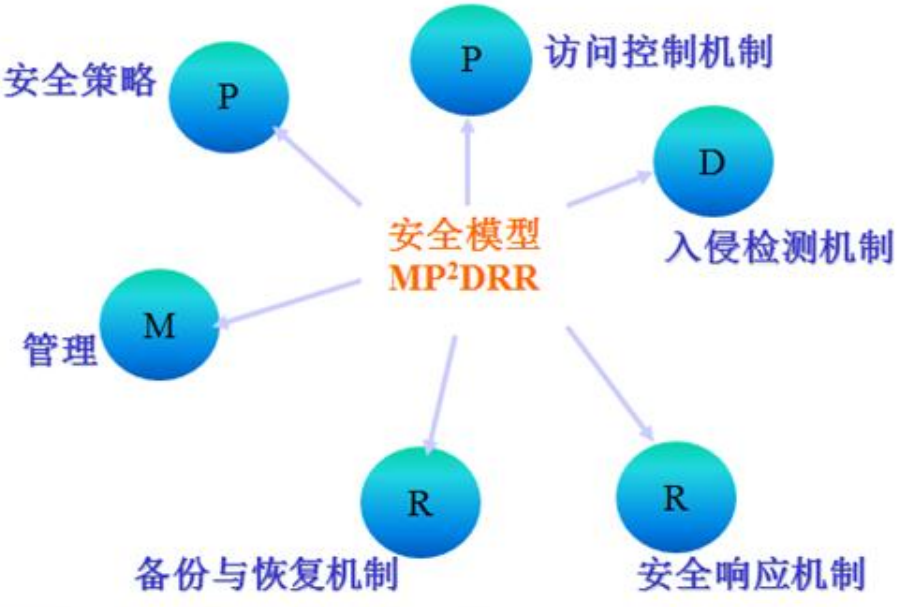
确保安全策略不与公司目标和实际活动相抵触

P2DR模型

以安全策略为核心的安全模型

ISS（Internet Security Systems InC.）提出

MP²DRR安全模型



四、信息安全的发展

（一）安全标准研究

1、美国 TCSEC(桔皮书)可信计算机系统评估准则。1985 年由 美国国防部制定。分为 4 个方面:安全政策、可说明性、 安全保障和文档，四类七个等级。

2、CC(通用准则)、安全管理标准 ISO17799 等；

3、1999 年 10 月我国颁布了《计算机信息系统安全保护等级划分准则》，将计算机安全保护划分为用户自主保护、系统审计保护、安全标记保护、结构化保护、访问验证保护五个级别

TCSEC

类别	级别	名称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构 较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

（二）OSI 信息安全体系结构

1989 颁布，确立了基于 OSI/RM 的信息安全体系结构

五大类安全服务

鉴别、访问控制、机密性、完整性、抗否认

八类安全机制

加密、数字签名、访问控制、数据完整性、

鉴别交换、业务流填充、路由控制、公证）

OSI 安全管理

ITU X.800, 1991 年颁布

（三）信息安全发展阶段

通信保密（COMSEC）：60-70 年代
　　信息保密
信息安全（INFOSEC）：80-90 年代
　　机密性、完整性、可用性、不可否认性
信息保障（IA）：90 年代-至今
　　对整个信息和信息系统进行动态保护与防御

华图网校
V.HUATU.COM
SINCE 2001
乐享品质　高效学习

■ 华图网校介绍

华图网校（V.HUATU.COM）于2007年3月由华图教育投资创立，是华图教育旗下的远程教育高端品牌。她专注于公职培训，　目前拥有遍及全国各地500万注册用户，已成为公职类考生学习提高的专业门户网站。

华图网校是教育部中国远程教育理事单位。她拥有全球最尖端高清录播互动技术和国际领先的网络课程设计思想，融汇华图教育十余年公职辅导模块教学法，凭借强大师资力量与教学资源、利用教育与互联网的完美结合，真正为考生带来“乐享品质”的学习体验，通过“高效学习”成就品质人生。

华图网校课程丰富多元，涵盖公务员、事业单位、招警、法院、检察院、军转干、选调生、村官、政法干警、三支一扶、乡镇公务员、党政公选等热门考试、晋升及选拔。同时，华图网校坚持以人为本的原则，不断吸引清华、北大等高端人才加入经营管理，优化课程学习平台，提升用户体验，探索网络教育新技术和教学思想，力争为考生提供高效、个性、互动、智能的高品质课程和服务。

华图网校将秉承“以教育推动社会进步”的使命，加快网站国际化进程，打造全球一流的网络学习平台。

我们的使命：以教育推动社会进步

我们的愿景：德聚最优秀人才，仁就基业长青的教育机构

我们的价值观：诚信为根、质量为本、知难而进、开拓创新。

■ **咨询电话：400-678-1009**
■ **听课网址：v.huatu.com（华图网校）**