保密安全与密码技术

第一讲　　绪论

- 36课时
- 考察方式：开卷考试或者论文（60%）
- 平时作业：小组讨论3次（30%）
- 考勤：10%
- 参照书：
  - 《网络安全与保密》胡建伟，西安电子科技大学出版社
  - 《网络信息安全技术》周明全，西安电子科技大学出版社
  - 《应用密码学-协议、算法与C源程序》（美）Bruce Schneier，吴世忠，祝世雄，张文政等译，机械工业出版社
  - 《计算机密码学》（第3版） 卢开澄著，清华大学出版社
- 答疑：每七天二15：00-16：30北教6-219

主要内容

- 绪论
- 密码学基础
- 网络安全应用基础
- 虚拟专用网VPN
- 公钥基础设施PKI及身份认证
- 访问控制与安全审计
- 防火墙技术
- 入侵检测系统IDS
- 病毒与数据安全
- 安全评估与安全管理

绪论

- 信息安全的有关概念
- 信息安全的层次构造
- 安全威胁、漏洞和攻击
- 信息安全的有关技术
- 网络安全模型

信息安全的有关概念

- 安全？
- 别墅的保护措施：
  - 挂上窗帘：防止让人看见房子内的情况
  - 门上加锁：以免让小偷入内
  - 养大狼狗：把不受欢迎的人拒之门外
  - 警报系统：有人强行闯进时发声警报
  - 带电围墙、设置专业保安人员等进一步措施。
- 我们的信息安全和网络安全也是相同的设计理念，保护我们的信息和资源。

信息安全的有关概念

- 安全的定义
  - “安全”一词的基本含义为，“远离危险的状态或特征”或“主观上不存在威胁，主观上不存在恐惊”。
- 信息的定义
  - 广义上讲，信息是从调查、研究和教育中取得的知识，是情报、新闻、事实、数据，是代表数据的信号或字符，是代表物质的或精神的经验信息及经验数据、图片。
  - 《信息科学原理》一书中以为，信息是事物运动的状态与方式，是物质的一种属性。
  - 信息不同于消息，消息只是信息的外壳，信息则是消息的内核
  - 信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容
  - 信息不同于数据，数据是统计信息的一种形式，一样的信息也能够用文字或图像来表述
  - 信息还不同于情报和知识。

信息安全的有关概念

- 信息安全的定义
  - 国内：
    - 国内学者：“信息安全保密内容分为：实体安全、运营安全、数据安全和管理安全四个方面。”
    - 我国计算机信息系统安全专用产品分类原则给出的定义：“涉及实体安全、 运营安全和信息安全三个方面。”
    - 国家信息安全要点试验室给出的定义：“信息安全涉及到信息的机密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。”

信息安全的有关概念

- 信息安全的定义
  - 国际：
    - BS7799信息安全管理原则：“信息安全是使信息防止一系列威胁，保障商务的连续性，最大程度地降低商务的损失，最大程度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”
    - 美国国家安全局：“ 信息安全仅表达信息的机密性，在国防部用‘信息保障’来描述信息安全。它涉及5种安全服务，涉及机密性、完整性、可用性、真实性和不可抵赖性。”
    - 国际原则化委员会：“为数据处理系统而采用的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶尔的或恶意的原因而遭到破坏、更改、显露”。这里面既涉及了层面的概念，其中计算机硬件能够看作是物理层面，软件能够看作是运营层面，再就是数据层面；又涉及了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

信息安全的有关概念

- 信息安全的定义
  - 纵观从不同的角度对信息安全的不同描述，能够看出两种描述风格：
    - 一种是从信息安全所涉及层面的角度进行描述，大致上涉及了实体（物理）安全、运营安全、数据（信息）安全；
    - 一种是从信息安全所涉及的安全属性的角度进行描述，大致上涉及了机密性、完整性、可用性。
  - 信息安全是预防对知识、事实、数据或能力非授权使用、误用、篡改或拒绝使用所采用的措施。维护信息本身的安全就要抵抗对信息的安全威胁。

信息安全的有关概念

- 信息安全的任务
  - 保护信息财产，以预防偶尔的或未授权者对信息的恶意泄露、修改和破坏，从而造成信息的不可靠或无法处理等。这么能够使得我们在最大程度地利用信息为我们服务的同步而不招致损失或使损失最小
- 信息安全的要求
  - 完整性（Integrity）
  - 保密性（Confidentiality）
  - 可用性（Availability）
  - 不可否定性（Non-repudiation）
  - 可控性（Controllability）

信息安全的层次构造

- 三个层次
  - 物理安全
  - 安全控制
  - 安全服务
- 物理安全
  - 自然灾害
  - 电磁辐射
  - 操作失误

信息安全的层次构造

- 安全控制
  - 操作系统安全控制
  - 网络接口模块的安全控制
  - 网络互连设备的安全控制
- 安全服务
  - 安全机制
  - 安全连接
  - 安全协议
  - 安全策略

安全威胁、漏洞和攻击

- 安全威胁
  - 信息安全威胁就是指某个人、物、事件或概念对信息资源的保密性、完整性、可用性或正当使用所造成的危险。攻击就是对安全威胁的详细体现。虽然人为原因和非人为原因都能够对通信安全构成威胁，但是精心设计的人为攻击威胁最大
  - 威胁是一种潜在的攻击，是一种还没有发生的安全事件。
  - 威胁定义为对缺陷的潜在利用。这些缺陷能够造成非授权访问、信息泄露、资源耗尽等破坏。

安全威胁、漏洞和攻击

- 安全威胁
  - 信息泄露
  - 破坏信息的完整性
  - 拒绝服务
  - 非法使用
  - 窃听
  - 业务流分析
  - 假冒
  - 旁路控制
  - 授权侵犯
  - 特洛伊木马
  - 陷阱门
  - 抵赖
  - 重放攻击
  - 计算机病毒

安全威胁、漏洞和攻击

- 安全威胁的动机
  - 工业、商业间谍
  - 经济、政治利益驱使
  - 报复或者引人注意
  - 恶作剧
  - 无知

安全威胁、漏洞和攻击

- 安全威胁途径
  - 人员不慎：一种授权的人为了钱或利益，或因为粗心，将信息泄露给一种非授权的人。
  - 媒体废弃：信息被从废弃的磁的或打印过的存储介质中取得。
  - 物理侵入：侵入者经过绕过物理控制而取得对系统的访问；
  - 窃取：主要的安全物品，如令牌或身份卡被盗；
  - 业务欺骗：某一伪系统或系统部件欺骗正当的顾客或系统自愿地放弃敏感信息。

安全威胁、漏洞和攻击

- 安全漏洞
  - 安全漏洞是指系统或者网络中存在的安全弱点，能够被入侵者利用的安全缺口。主要体目前下列几种方面：
    - 操作系统安全的脆弱性
    - 计算机网络安全的脆弱性
    - 数据库管理系统安全的脆弱性
    - 软件安全漏洞
    - 不兼容使用安全漏洞

安全威胁、漏洞和攻击

- 安全攻击
  - 攻击是指任何非授权行为。
  - 攻击的法律意义：攻击仅发生在入侵行为完全完毕而且入侵者已经在目的网络内。
  - 教授观点：可能使一种网络受到破坏的全部行为都定义为攻击。
  - 攻击主要分为：被动攻击和主动攻击

安全威胁、漏洞和攻击

- 攻击的目的
  - 攻击目的一般有两类：系统和数据。
  - 系统型攻击：30%
  - 数据型攻击：70%
  - 一种完整的安全方案不但能预防系统类攻击，也能预防数据型攻击；既能处理系统安全，又能处理数据安全的问题。

安全威胁、漏洞和攻击

- 攻击过程
  - 攻击主要有三个环节：信息搜集、弱点探测与分析、实施攻击。
  - 信息搜集：踩点、窥视
  - 弱点探测与分析：操作系统漏洞、网络设置漏洞，通信协议漏洞等。
  - 实施攻击：寻找内部落脚点，实施攻击，最终清楚攻击痕迹。

安全威胁、漏洞和攻击

- 安全手段
  - 利用系统缺陷或“后门”软件
  - 利用顾客单薄的安全意识
  - 防火墙的安全隐患
  - 内部顾客的泄密和破坏
  - 网络监督和系统安全评估的缺乏
  - 制造口令攻击和拒绝服务
  - 利用WEB服务的缺陷