黑客攻防

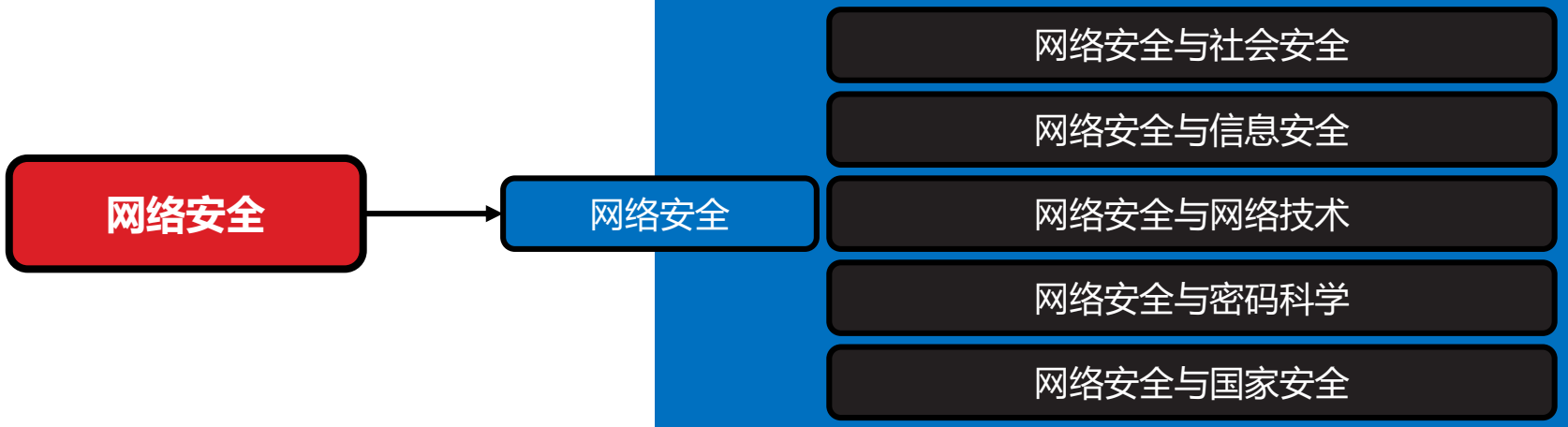
网络安全概述

Unit01

内容

上午	09:00 ~ 09:30	网络安全
	09:30 ~ 10:20	网络威胁
	10:30 ~ 11:20	研究范围
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	人员需求
	16:00 ~ 16:50	课程简介
	17:00 ~ 17:30	

网络安全


网络安全
网络安全
网络安全与社会安全
网络安全与信息安全
网络安全与网络技术
网络安全与密码科学
网络安全与国家安全

网络安全

网络安全与社会安全

- 计算机网络的虚拟社会和现实社会之间在很多方面都存在着“对应”关系
- 现实社会中的人与人在交往中形成了复杂的社会与经济关系，这些关系以数字化的形式延续到网络社会之中
- 网络安全是现实社会安全的反映
- 网络安全问题实际上是个社会问题，光靠技术来解决这些问题是不可能的
- 网络安全是一个系统的社会工程，它涉及技术、政策、道德与法律法规等许多方面

知识讲解

网络安全与信息安全

- 用户的各种信息被保存在不同类型的应用系统之中
- 各种类型的应用系统建立在不同的计算机系统之上
- 从运行应用系统的大型服务器、服务器集群到个人用户的计算机、手机等智能设备，都是以固定或移动的方式接入计算机网络中的
- 用户信息的安全取决于应用系统的安全，应用系统的安全取决于计算机的安全，而计算机的安全取决于网络的安全
- 网络安全是信息安全的基础，不能保证网络的安全性，信息的安全性也就无从谈起

知识讲解

网络安全与网络技术

- 形形色色的网络技术在造福于人类社会的同时，也成为黑客和居心不良者用于实施犯罪的工具
- 每一项网络技术的发明都是一把双刃剑，在为人们的生活和工作带来便捷的同时，也增加了人们遭受网络攻击、网络诱骗、信息窃取的风险
- 成功的网络技术必须是功能性与安全性的统一。网络安全问题不仅仅是网络安全工程师需要面对的问题，也是每一位网络技术研发和管理者都必须考虑的问题

知识讲解

网络安全与密码科学

- 密码学是信息安全研究的重要工具，密码学在网络安全领域有很多重要应用
- 密码学是数学的一个分支，数学是完美的，但人类社会却无法用数学准确地表达
- 网络安全问题归根到底是人与人、人与机器之间的关系问题，而人是有感情和欲望的，是不稳定的，甚至是难以理解的，这与精确并严格遵循逻辑的数学格格不入
- 历史的经验已然证明，安全性的弱点与数学毫无关系，它们存在于硬件、软件、网络和人的身上。安全性是一个过程，而不是一个产品
- 密码学是研究网络安全所必需的一个重要工具和方法，但是网络安全所涉及的领域，比密码学本身所能解决的问题要广泛得多

知识讲解

网络安全与国家安全

- 网络安全对国家安全的影响
  - 2001年的阿富汗战争中，美国为了配合武装战争，实施了包括黑掉对方银行账户等在内的多种信息战方法
  - 近年来有记录显示，很多中东和其它地区的黑客正不遗余力地试图黑掉美国发电厂的网站，甚至进入美国和欧洲的核电站控制系统
  - 能源电力、通信网络、城市交通、航空管制、卫星定位、智能楼宇等越来越多与国计民生休戚相关的业务系统构建于计算机网络之上，今后很可能成为黑客乃至敌对国家发动网络战争的攻击目标
  - 一场成功的网络战争关键在于攻防计划和系统弱点。攻防计划包括人员、技术、工具以及网络武器等条件的准备，而系统弱点则取决于双方对网络的依赖程度以及对网络安全的重视程度

知识讲解

网络安全与国家安全

- 信息时代国家安全战略重点的转移
  - 美国和一些发达国家都已经将防范和应对攻击与破坏关键信息基础设施作为信息时代国家安全战略的重点
  - 从2006年开始，美国、英国等多个国家已先后举行了数次代号为“网络风暴”的大规模网络战争演习，以全面检验国家的网络安全和应急能力。演习模拟了政府机构、银行、通信、信息、能源、航空与铁路运输等多个重要行业的网络系统遭受联合攻击时，网络安全专家应对攻击的处理能力。演习的目的就是针对各部门、各企业的网络安全漏洞，检验它们的网络应急计划和遭袭击后迅速恢复的能力，检验国家的网络安全状况和应急处理协调能力

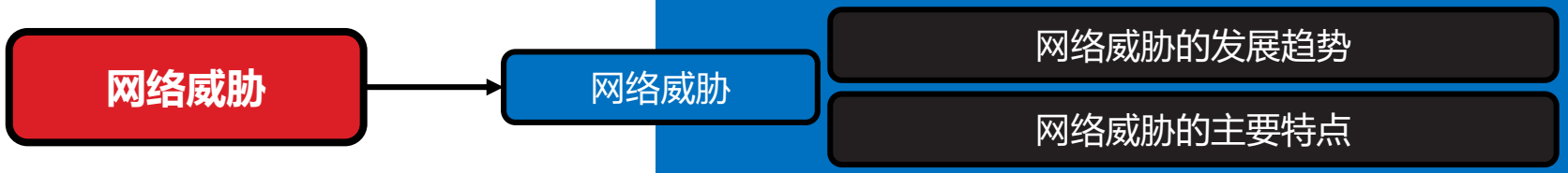
知识讲解

网络安全与国家安全

- 国际范围内互联网应用的最新动向
  - 自2009年以来，美国政府在国家网络安全评估报告中率先指出，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一，美国国防部宣布成立“网络战”司令部，美国参议院提交议案，赋予总统在紧急状态下关闭互联网服务的权力，美国国土安全部获准招募1000名网络安全专家，美国政府要求全社会的机构和个人都参与到网络安保中来，从而将网络安全渗透到整个美国社会
  - 网络安全问题已经成为信息化社会的一个焦点问题。每个国家只有立足于本国，研究网络安全技术，培养网络安全人才，发展网络安全产业，才能构筑起适合本国国情的网络安全防范体系
  - 自主研发网络安全技术，发展网络安全产业是关系到一个国家国计民生与国家安全的重大问题。哪个国家不重视网络安全，它就必将在未来的国际竞争中处于被动和危险的境地

知识讲解

网络威胁



网络威胁

网络威胁的发展趋势

- 受经济利益驱动，网络攻击的动机已经从初期的恶作剧、显示能力、寻求刺激，逐步向有组织的犯罪方向发展，甚至形成有规模的跨国经济犯罪
- 网络罪犯正在逐步形成黑色产业链，网络攻击日趋专业化和商业化
- 网络犯罪活动的范围随着互联网的普及，逐渐从经济发达国家和地区向一些发展中国家和地区蔓延
- 网络攻击已经超出了传统意义上网络犯罪的概念，正逐步演变为某些国家或利益集团重要的政治和军事工具，甚至成为恐怖分子发动袭击的手段

知识讲解

网络威胁的主要特点

- 地下交易体系呈现专业化和商业化的趋势
  - 通过社交网站和假冒安全软件窃取用户敏感信息的事件明显增加
  - 在所有网络攻击中，约90%针对的是用户机密信息，如银行账户、信用卡信息等，这种攻击目前正呈增长趋势
- 智能手机成为新的攻击目标
  - 随着3G、4G乃至5G移动通信技术的发展，智能手机已经成为继个人电脑之后下一个网络攻击的目标。病毒制作者可以象制作Windows病毒一样，开发出针对Android和iOS等操作系统的病毒软件

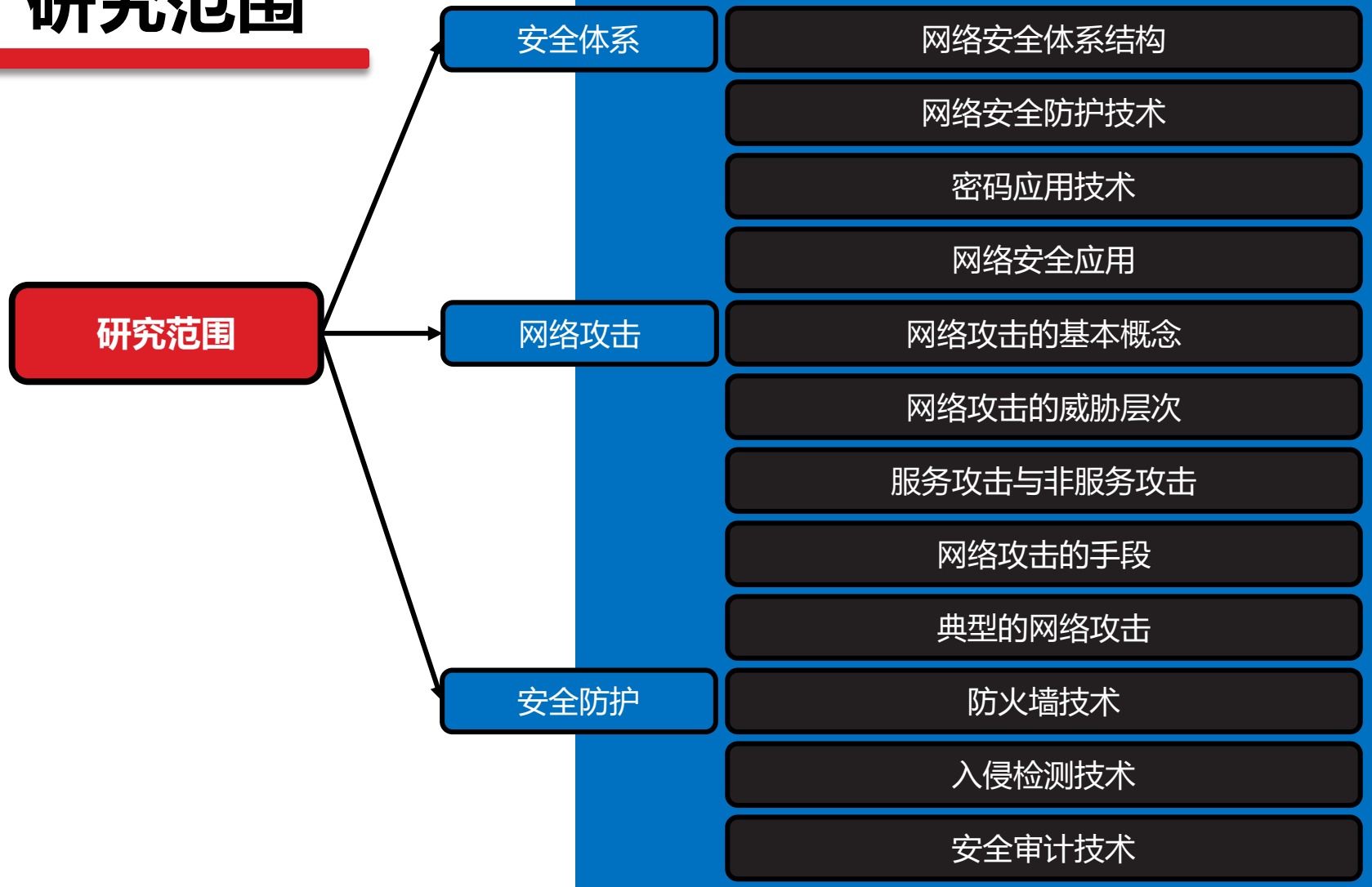
知识讲解

网络威胁的主要特点

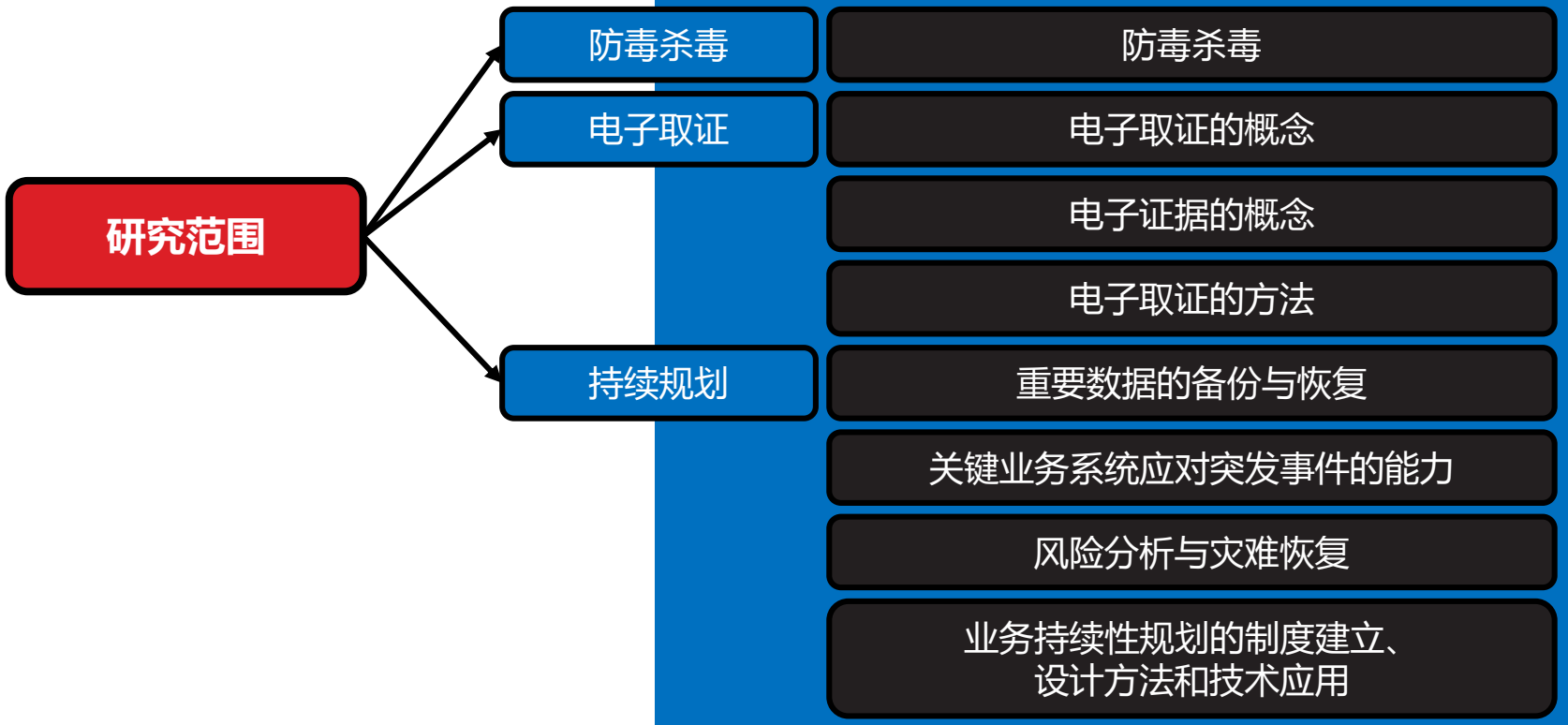
- 受网络病毒感染的网页数量和垃圾邮件数量持续攀升
  - 随着B/S架构和前端技术的日益流行，基于网页的应用渐渐取代了传统的专用客户端，但随之而来的是网页已经逐渐成为网络攻击的主要渠道，越来越多的用户会因为访问一些日常网站而受到感染
  - 在一般性商务和政务活动中，电子邮件服务已渐渐取代传统邮政服务，成为官方、半官方和非官方的首要信息沟通渠道，而在全部商业邮件当中，垃圾邮件的占比竟高达90%，且呈逐年攀升态势
- Web 2.0和搜索引擎服务成为网络黑客们攻击的重点
  - Web 2.0和搜索引擎为开发者用户提供了应用编程接口(API)，因此也成为黑客们攻击和利用的目标和途径。随着越来越多网络服务的推出，黑客们更倾向于利用Web API骗取用户信任，窃取用户信息

知识讲解

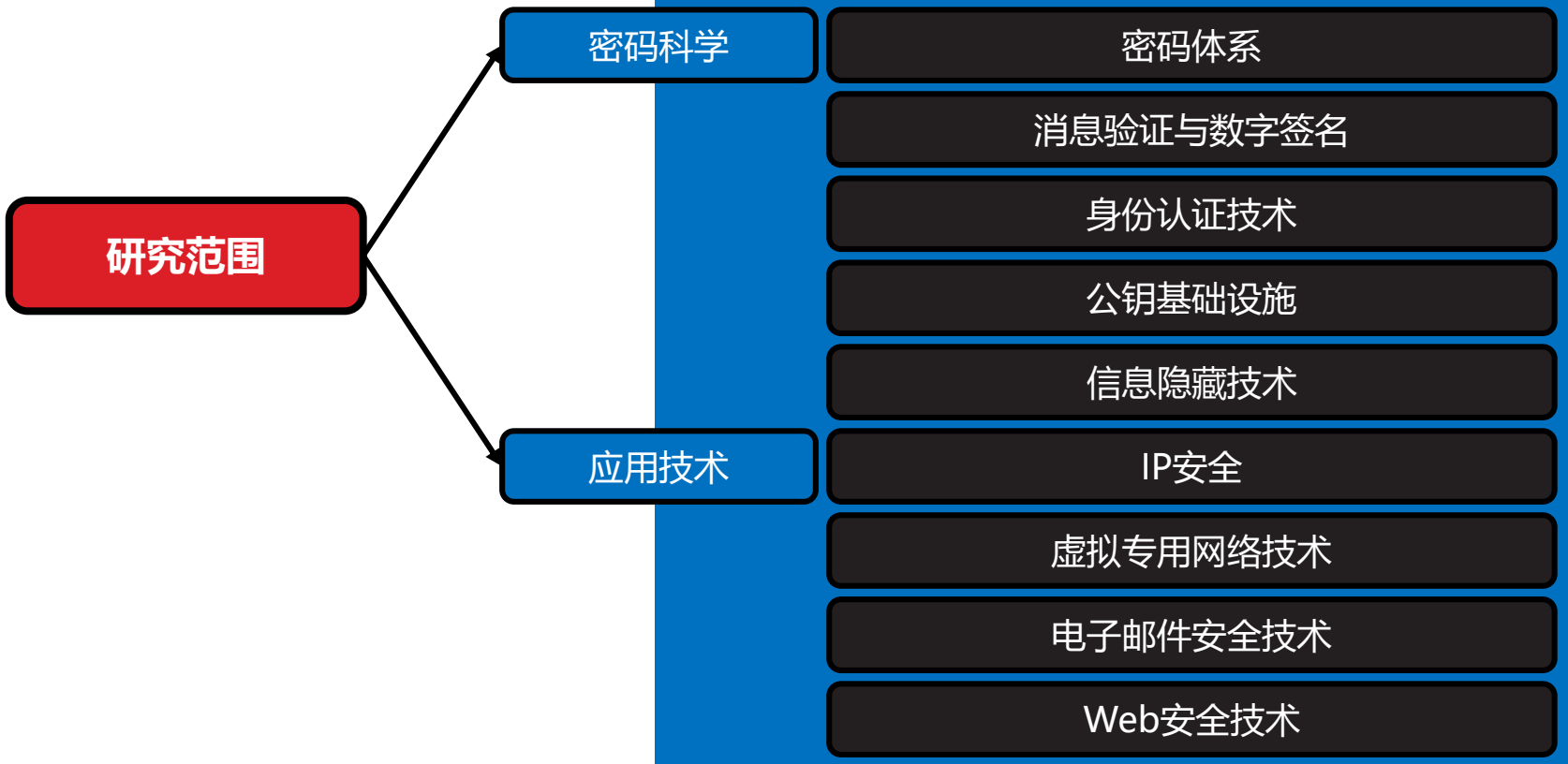
研究范围


研究范围
安全体系
网络安全体系结构
网络安全防护技术
密码应用技术
网络安全应用
网络攻击
网络攻击的基本概念
网络攻击的威胁层次
服务攻击与非服务攻击
网络攻击的手段
典型的网络攻击
安全防护
防火墙技术
入侵检测技术
安全审计技术

研究范围


研究范围
防毒杀毒
电子取证
持续规划
防毒杀毒
电子取证的概念
电子证据的概念
电子取证的方法
重要数据的备份与恢复
关键业务系统应对突发事件的能力
风险分析与灾难恢复
业务持续性规划的制度建立、
设计方法和技术应用

研究范围

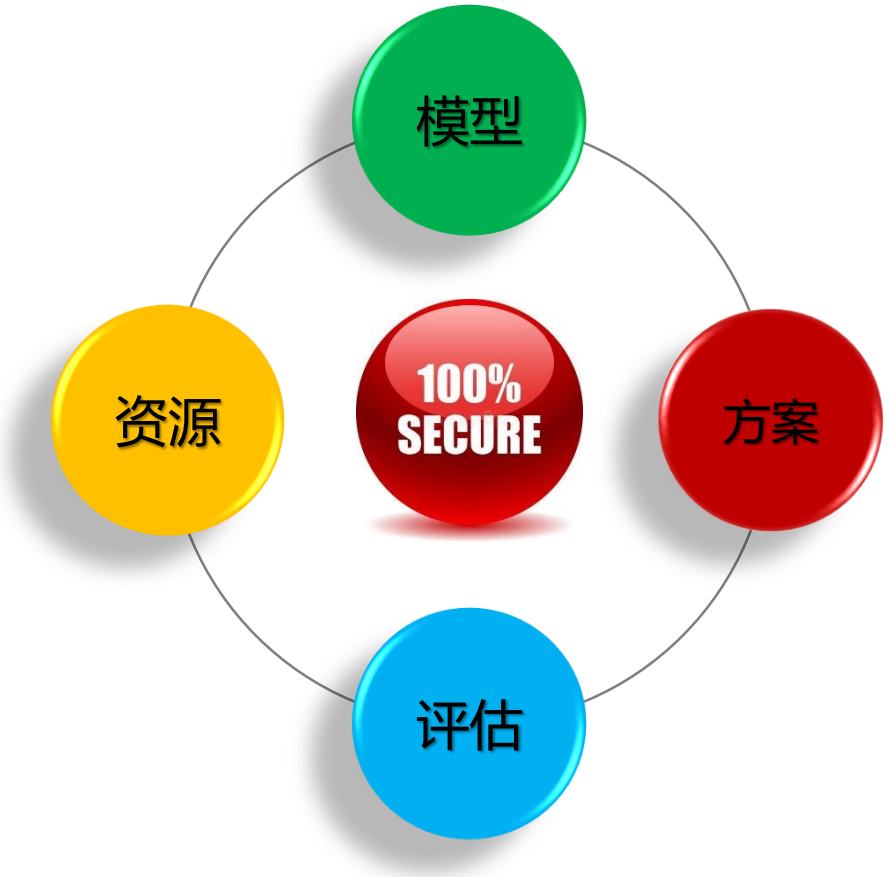

研究范围
密码科学
应用技术
密码体系
消息验证与数字签名
身份认证技术
公钥基础设施
信息隐藏技术
IP安全
虚拟专用网络技术
电子邮件安全技术
Web安全技术

安全体系

网络安全体系结构

- 根据对网络安全威胁的分析，确定需要保护的网络资源
- 根据对资源攻击者、攻击目的和手段及其所造成危害的分析，确定网络安全模型
- 根据网络安全模型的不同层次，确定网络安全解决方案
- 制定用于评估系统安全性的标准和方法，以此作为采取网络安全措施的依据

知识讲解



网络安全防护技术

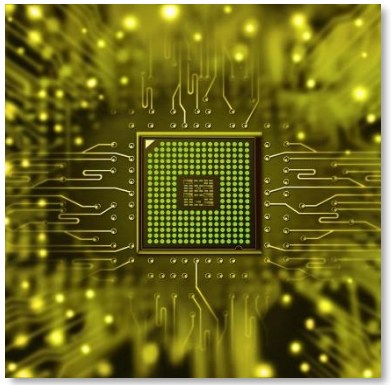
- 防火墙技术
- 入侵检测技术
- 防攻击技术
- 防病毒技术
- 安全审计技术
- 电子取证技术
- 业务持续性技术

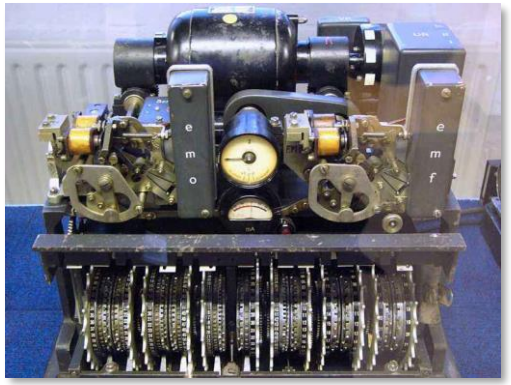
知识讲解

密码应用技术

- 对称密码技术
- 公钥密码技术
- 消息摘要技术
- 数字签名技术
- 信息隐藏技术
- 公钥基础设施技术

知识讲解





网络安全应用

- IP安全技术
- 虚拟专用网络技术
- 邮件安全技术
- Web安全技术
- 信息过滤技术

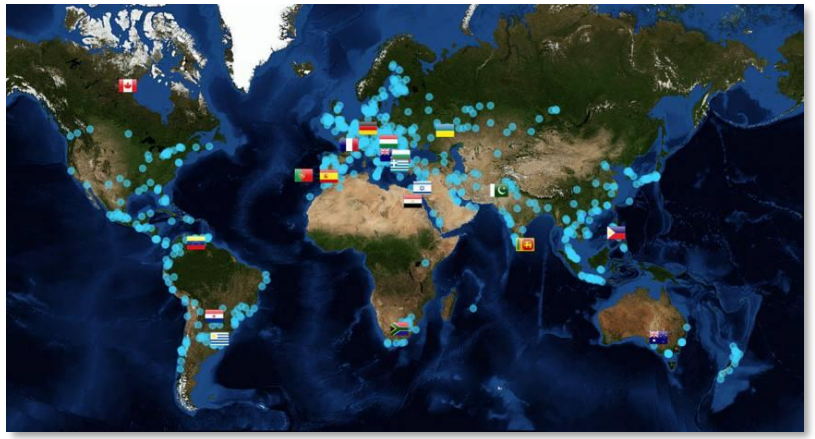
知识讲解

网络攻击

网络攻击的基本概念

- 作为网络安全领域的从业人员，必须对各种黑客攻击技术有充分且深入的研究。只有掌握了各种攻击方法和手段，才有可能有针对性地采取防范措施
- 法律意义上的网络攻击仅仅发生在入侵行为完全完成的时刻，且入侵者必须身处被攻击系统内部
- 对于网络安全管理者而言，一切可能导致网络系统遭受破坏的行为都可被视为攻击

知识讲解



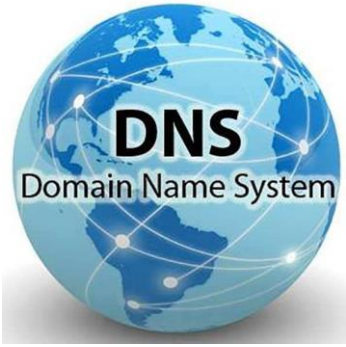
网络攻击的基本概念

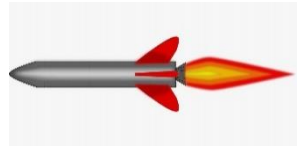
- 目前网络攻击大致可以分为：
  - 系统入侵类攻击：通过破坏主机和网络系统的安全防护机制，非法获取对主机系统的控制权。这类攻击又分为信息收集攻击、口令攻击和漏洞攻击等
  - 缓冲区溢出攻击：通过向程序的缓冲区写入超出其长度限制的内容，造成缓冲区溢出，破坏程序的堆栈结构，致使程序转而执行其它指令，最终令攻击者获得对程序的控制权
  - 欺骗类攻击：网络欺骗的主要类型包括IP欺骗、ARP欺骗、DNS欺骗、Web欺骗、电子邮件欺骗、源路由欺骗、地址欺骗和口令欺骗等
  - 拒绝服务攻击

知识讲解

网络攻击的威胁层次

- 网络攻击的威胁可以分为三个层次：
  - 攻击主干网络的威胁
    - 攻击主干路由器的威胁
    - 攻击DNS服务器的威胁
  - 攻击TCP/IP协议栈的威胁
  - 攻击网络应用的威胁





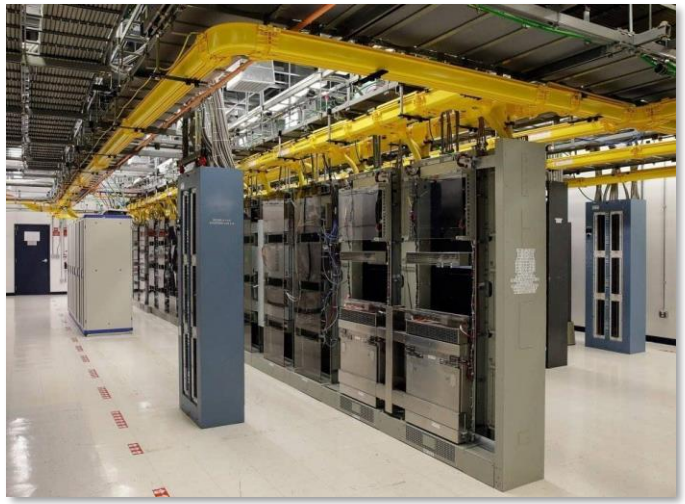
- 1997年7月，由于人为错误导致根域DNS服务器工作异常，致使互联网局部服务中断
- 2002年8月，黑客利用互联网主干网的ASN No.1信令漏洞，攻击了主干路由器、交换机和一些基础设施，造成了严重的后果
- 2002年10月，全球13台根域DNS服务器遭受大规模分布式拒绝服务(DDoS)攻击，其中9台服务器几近瘫痪

知识讲解

服务攻击与非服务攻击

- 服务攻击是指针对为网络提供某种特定服务的服务器发起的攻击。特定的网络服务包括电子邮件服务、Telnet服务、FTP服务、Web服务等
- 非服务攻击不针对具体的网络服务，而是对网络层或更低层级的协议发起攻击。攻击者通过各种方法攻击路由器、交换机等网络通信设备，令其工作严重阻塞或瘫痪

知识讲解



网络攻击的手段

- 网络攻击的手段层出不穷，截至目前可大致分为以下几类：
  - 欺骗型攻击
    - 口令欺骗攻击
    - IP地址欺骗攻击
    - ARP欺骗攻击
    - DNS欺骗攻击
    - 源路由欺骗攻击
  - 拒绝服务攻击
    - 资源消耗型攻击
    - 修改配置型攻击
    - 物理破坏型攻击
    - 服务利用型攻击
  - 信息收集攻击
    - 扫描攻击
    - 体系结构探测攻击
    - 利用信息服务攻击
  - 漏洞攻击
    - 网络协议漏洞攻击
    - 操作系统漏洞攻击
    - 应用软件漏洞攻击
    - 数据库漏洞攻击

知识讲解

典型的网络攻击

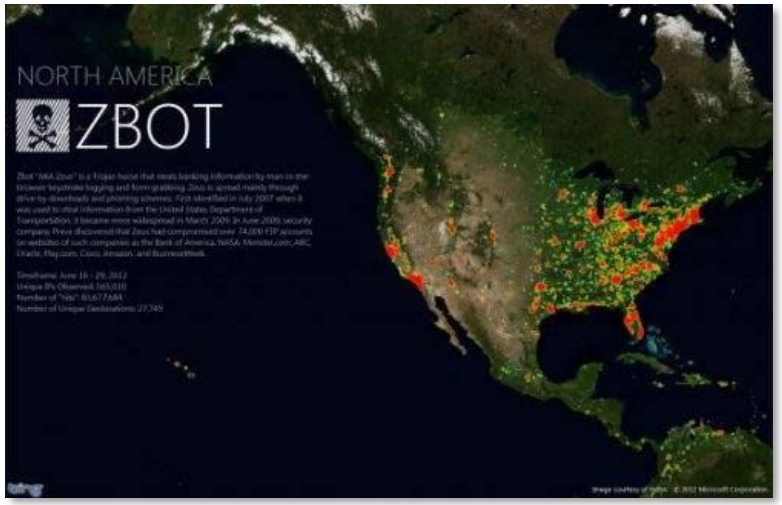
- 拒绝服务攻击
  - 拒绝服务(Denial of Service, DoS)攻击主要是通过消耗网络系统有限的、不可恢复的资源，使合法用户应该获得的服务质量出现下降或者遭到拒绝。拒绝服务攻击的目的不是入侵系统或者更改数据，而是使系统无法响应合法的服务请求
    - 资源消耗型攻击
    - 修改配置型攻击
    - 物理破坏型攻击
    - 服务利用型攻击

知识讲解

典型的网络攻击

- 分布式拒绝服务攻击
  - 分布式拒绝服务(Distributed Denial of Service, DDoS)攻击的攻击者利用多台分布在不同位置的代理主机，同时向一个目标发动拒绝服务攻击，令其迅速陷入瘫痪

知识讲解

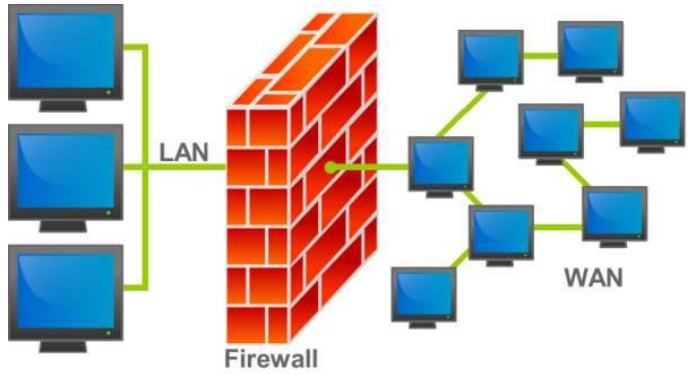


安全防护

防火墙技术

- 设置防火墙的目的是保护内部网络资源不被外部非授权用户使用，防止内部系统受到外部非法用户的攻击
- 防火墙通常位于内部网络和外部网络之间
- 防火墙的主要功能包括：
  - 检查所有从外部网络流向内部网络的数据包
  - 检查所有从内部网络流向外部网络的数据包
  - 限制所有不符合安全策略要求的数据包通过
  - 具备足够的抗攻击能力，保证其自身的安全

知识讲解



防火墙技术

- 防火墙的两大基本构件：
  - 包过滤路由器：按照系统内部设置的分组过滤规则，即访问控制列表，检查每个分组的源IP地址、目的IP地址、协议类型、IP选项、源TCP端口号、目的TCP端口号以及TCP ACK标识等网络层和传输层包头信息，以决定是否转发该分组
  - 应用级网关：以存储转发的方式，检查和确定请求网络服务的用户身份是否合法，以决定是转发还是丢弃该服务请求。应用级网关的优点是可以针对某一特定的网络服务，并能在应用层协议的基础上分析、转发服务请求和响应，同时提供日志记录功能
- 防火墙是一个由软件和硬件组成的系统，针对不同的安全策略和防护目的，防火墙系统的配置和实现方式存在很大差别。实际的防火墙系统通常是以包过滤路由器和应用级网关作为基本单元，复合为多级结构和多种组态

知识讲解

入侵检测技术

- 什么是入侵检测系统
  - 入侵检测系统(Intrusion Detection System, IDS)是对计算机和网络资源的恶意使用行为进行识别的系统，旨在监测和发现可能存在的潜在攻击行为，包括来自系统外部的入侵行为和来自内部用户的非授权行为，并采取相应的防护措施
- James Anderson对网络入侵的定义是：
  - 潜在的、有预谋的、未经授权的服务操作，目的是使网络系统不可靠或无法使用
- 入侵检测系统的主要功能：
  - 监控、分析用户和系统的行为
  - 检查系统的配置和漏洞
  - 评估重要的系统和数据文件的完整性
  - 通过对异常行为的统计分析，识别攻击类型，并向网络管理人员报警
  - 对操作系统进行审计、跟踪和管理，识别违反授权的用户活动

知识讲解

入侵检测技术

- 入侵检测系统作为一种主动式、动态的防御技术迅速发展起来，成为当前网络安全领域中一个新的热点。入侵检测系统通过动态探查网络内的异常情况，及时发出警报，有效弥补了其它静态防御技术的不足。入侵检测系统正在成为对抗网络攻击的关键技术，其未来的发展方向是智能化、分布式、实时性的网络入侵防御系统
- 入侵检测系统的分类
  - 根据体系结构的不同，可将入侵检测系统分为：
    - 基于主机的入侵检测系统：集中式入侵检测
    - 基于网络的入侵检测系统：分布式入侵检测
      - 分布式入侵检测系统
      - 大规模分布式入侵检测系统

知识讲解

入侵检测技术

- 入侵检测系统的分类
  - 根据检测对象的不同，可将入侵检测系统分为：
    - 针对目标的入侵检测系统
    - 针对应用的入侵检测系统
  - 根据工作方式的不同，可将入侵检测系统分为：
    - 在线式入侵检测系统：
      实时审计分析网络数据包
    - 离线式入侵检测系统：
      非实时，事后分析审计事件，从中检测入侵行为

知识讲解

安全审计技术

- 安全审计是对用户使用网络和计算机所有活动的记录、分析和审查，并以此作为发现安全隐患，追溯攻击源、辨别攻击类型、评估攻击危害、搜集网络犯罪证据的依据
- 安全审计系统的要求：
  - 用于安全审计的信息必须被有选择地保留和保护，与安全有关的活动能够被追溯到责任方
  - 能够选择和记录与安全有关的重要信息，以便将审计的开销减至最小，提高安全审计的效率
  - 能够创建和维护审计数据，保证用于安全审计的数据记录不被删除、修改和非法访问

知识讲解

安全审计技术

知识讲解

- 安全审计系统的功能：
  - 自动响应
  - 事件选择
  - 事件生成
  - 事件存储
  - 审计分析
  - 审计预览
- 安全审计的信息来源：
  - 网络设备及防火墙日志
    - 只记录自身的运转情况和简单的违规操作信息
    - 流量分析能力弱，不足以作为安全审计的依据
    - 使用内存记录日志，空间有限，经常需要覆盖
  - 操作系统日志
    - 过于零散而庞杂，人工提取安全信息十分困难
    - 安全级别不够高，被人为修改的可能性比较大

防毒杀毒

防毒杀毒

- 恶意传播的代码(Malicious Mobile Code, MMC)，是一种软件程序，它被设计为可从一台计算机传播到另一台计算机，从一个网络传播到另一个网络，意在于网络和系统管理员不知情的情况下，对网络和系统进行故意地破坏
- 恶意传播的代码包括：
  - 病毒：通过修改宿主文件或引导扇区复制自身，被感染文件还能感染其它文件
  - 木马：既不复制自身也不会感染其它文件，在用户不知情的情况下，被装入用户的计算机并试图控制该计算机或窃取用户的个人信息
  - 蠕虫：不依赖其它文件或引导扇区作为宿主，完全依靠自身进行自我复制。蠕虫典型的传播方式是利用广泛使用的应用程序，如电子邮件、聊天室等
  - 攻击脚本、垃圾邮件、流氓软件、恶意互联网代码等

知识讲解

防毒杀毒

- 根据传染媒介的不同，可将病毒分为：
  - 引导型病毒
  - 文件型病毒
  - 复合型病毒
- 根据感染方式的不同，可将病毒分为：
  - 源码型病毒
  - 入侵型病毒
  - 系统型病毒
- 根据危害程度的不同，可将病毒分为：
  - 良性病毒
  - 恶性病毒

知识讲解

电子取证

电子取证的概念

- 电子取证是指通过对被入侵计算机或网络设备的扫描和破解，重构入侵的步骤，获取、保存、分析和出示具有法律效力的电子证据的全过程

知识讲解

电子证据的概念

- 电子证据是指在法庭上可能作为证据的以二进制形式存储或传输的信息
- 与传统意义上的证据一样，电子证据必须是可信的、准确的、完整的、合法且能够被法庭接受的
- 但与传统意义上的证据相比，电子证据又有其特殊性：
  - 多样性：电子证据可以存储在计算机的内存、硬盘、软盘、光盘、磁带等多种介质中，可以表现为文本、图形、图像、音频、视频等多种形式
  - 准确性：排除人为蓄意破坏等干扰因素，电子证据是准确的，能够真实地反映事件的过程和细节
  - 客观性：电子证据不受人的感情和经验等主观因素的影响，更能表现客观事实的本来面貌
  - 易变性：电子证据通常非常容易被修改

知识讲解

电子取证的方法

- 静态取证
  - 静态取证是在案发之后或已经造成严重后果之后对现场取证：
    - 缺乏实时性和连续性，这样的证据在法庭上缺乏足够的说服力
    - 如果作案者已将证据销毁，则可能无法起诉
    - 事后处理，即便作案者能够被绳之以法，但其危害已然造成
- 动态取证
  - 动态取证通过对攻击行为的实时监控，在启动应急响应，评估危害程度，采取相应措施的同时，详细记录犯罪过程以作为呈堂证供：
    - 网络攻击一般要经过嗅探、入侵、破坏、掩盖足迹等多个步骤
    - 网络安全系统可借助入侵检测技术和“蜜罐”技术完成针对每个攻击步骤的同步实时取证

知识讲解

持续规划

重要数据的备份与恢复

- 在实际的网络运行环境中，数据备份与恢复功能非常重要。数据一旦丢失，特别是重要数据，可能会给用户造成无可挽回的损失
- 重要数据的备份需要解决以下几个基本问题：
  - 选择备份设备
  - 选择备份程序
  - 建立备份制度

知识讲解

关键业务系统应对突发事件的能力

- 网络安全领域中的突发事件是指由于网络基础设施的服务中断导致组织业务流程的非计划性中断。具体原因包括：
  - 洪水、飓风、地震等自然灾害
  - 战争、恐袭、政变等人为动乱
  - 网络攻击、病毒和组织内破坏
- 这些突发事件的出现，有可能导致网络和计算机系统的硬件和软件损坏，密钥和数据丢失，最终造成组织业务流程的非计划性中断
- 针对可能发生的突发事件，必须提前做好预案，建立必要的应急响应机制，力图将突发事件对关键业务系统所造成的影响减至最小

知识讲解

风险分析与灾难恢复

- 业务持续性规划既包括事前的风险分析，也包括事后的灾难恢复，这是一个统一的规划方法学问题

知识讲解

业务持续性规划的制度建立、设计方法和技术应用

- 业务持续性规划不是一个纯技术问题，它是一个从制度建立到设计方法，直至技术应用的系统工程

知识讲解

密码科学

密码体系

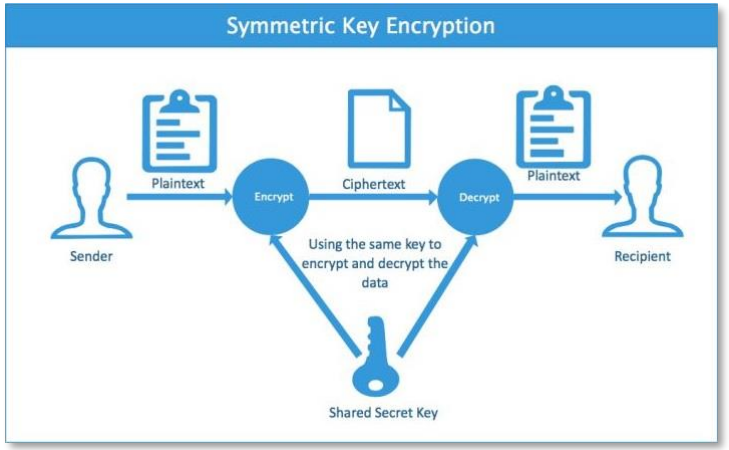
- 密码学包括：
  - 密码编码学：通过特定编码规则(算法)和秘密数值(密钥)对信息进行伪装和隐藏
  - 密码分析学：从被伪装和隐藏的信息中破译所用编码规则(算法)和秘密数值(密钥)
- 密码体系的两大构成要素：
  - 加解密算法
    - 加密算法：将明文伪装成密文的信息变换规则
    - 解密算法：将密文还原成明文的信息变换规则
  - 密钥：密码算法中的可变参数。在算法一定的条件下，改变了密钥也就改变了明文与密文之间的函数对应关系
- 现代密码学的一个基本原则是，一切秘密寓于密钥之中。密码体系中的加解密算法通常是公开的，真正需要保密的是密钥

知识讲解

密码体系

- 对于同一种加密算法，密钥的位数越长，密钥空间越大，破译难度也就越大，安全性越高。但是密钥越长，加解密运算的时间也越长，通常需要在安全与性能之间做出权衡
- 根据加密和解密所用密钥对称性的不同，可将密码体系分为：
  - 对称密码体系：加密和解密使用完全相同的密钥，该密钥在使用过程中必须严格保密
  - 公钥密码体系：加密和解密使用两把不同的密钥，其中用于加密的密钥可以公开，称为公钥，用于解密的密钥必须保密，谓之私钥

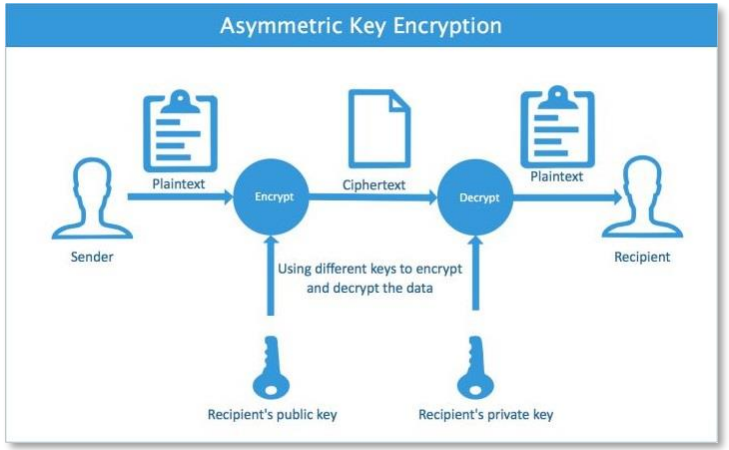
知识讲解



密码体系

- 公钥密码体系相比于对称密码体系：
  - 优点
    - 密钥管理简单，N个用户之间只需要维护N对密钥
    - 密钥无需共享，用于解密的私钥无需发往任何地方
  - 缺点
    - 算法相对复杂，加解密速度比较慢，一般不用于对数字内容的加密，而仅用于：
      - 对对称密钥加密
      - 防篡改、防抵赖
      - 发送端身份认证

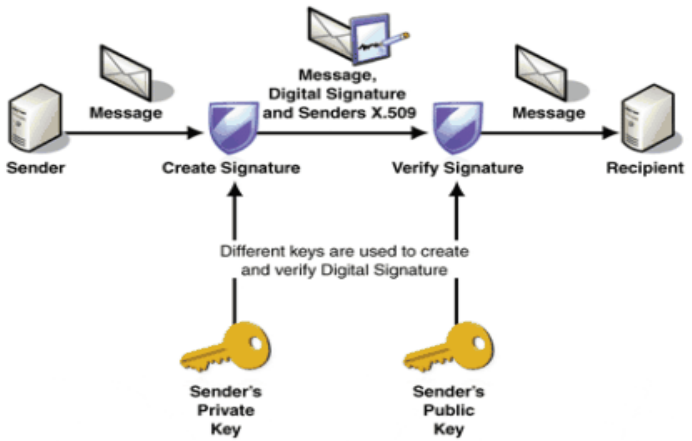
知识讲解



消息验证与数字签名

知识讲解

- 消息验证与数字签名的过程：
  - 发送方做数字签名：
    - 通过特定的散列函数对所要发送的数字内容计算其消息摘要
    - 通过其所持有的私钥对该消息摘要进行加密，得到数字签名
    - 将数字内容连同数字签名一起发送给接收方
  - 接收方做消息验证：
    - 通过相同的散列函数对所接收到的数字内容计算其消息摘要
    - 通过与发送方所持有的私钥配对的公钥对数字签名进行解密
    - 将计算所得与解密所得消息摘要进行比较，二者应完全相同



消息验证与数字签名

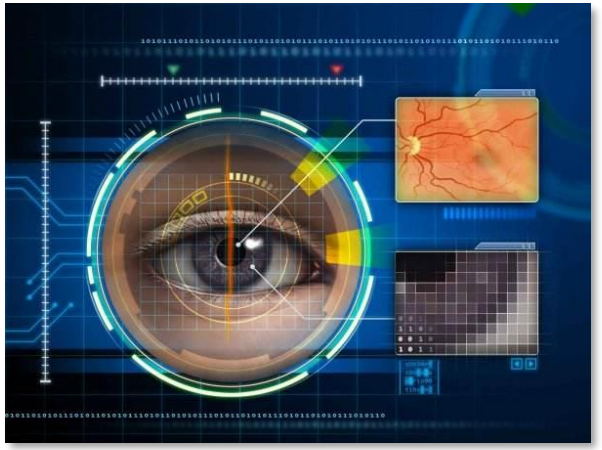
- 消息验证与数字签名的作用：
  - 防篡改：如果数字内容在传输过程中遭到篡改，接收方根据被篡改过的数字内容计算得到的消息摘要，应与解密数字签名得到的原始消息摘要完全不同
  - 防抵赖：用于数字签名的公钥是完全公开的，接收方可将所收到的数字内容、数字签名连同解密公钥一并交由可信任第三方，第三方一旦确认消息验证通过，即可证实发送方必然是对应加密私钥的持有者
  - 发送端身份认证：接受方通过与发送方加密私钥相对应的解密公钥解密发送方的数字签名，只要消息验证通过，即可对发送方的身份进行确认，因为除与该解密公钥相对应的加密私钥的持有者外，再没有其它人能够生成如此密文

知识讲解

身份认证技术

- 身份认证可以通过以下三种基本途径之一或它们的组合来实现：
  - 所知认证：被认证者所掌握的密码、口令等身份识别信息
    - 密码、口令等身份识别信息可能被泄露
  - 所有认证：被认证者所持有的身份证、护照、信用卡、社保卡等身份标志物
    - 身份证、护照、信用卡、社保卡等身份标志物可能被遗失或伪造
  - 特征认证：被认证者所特有的指纹、声纹、容貌、虹膜、DNA等生物统计特征
    - 指纹、声纹、容貌、虹膜、DNA等生物统计特征不易遗失而又难于伪造，可信度高，是目前网络环境中最简单而安全的身份认证方法

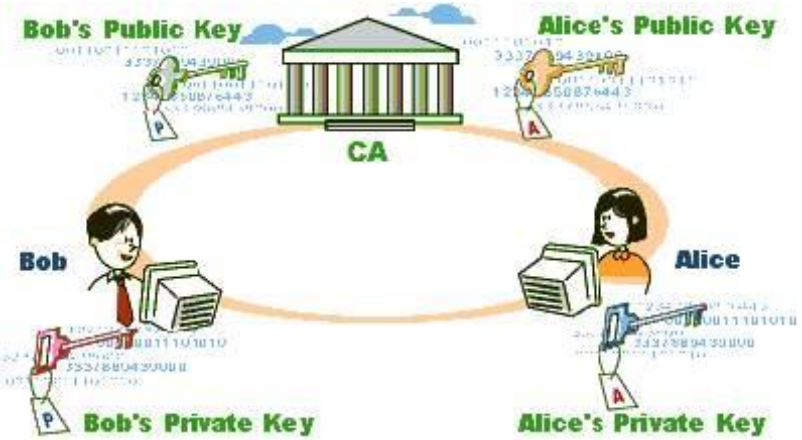
知识讲解



公钥基础设施

- 公钥基础设施(Public Key Infrastructure, PKI)是构建于公钥加密和数字签名技术基础之上的安全服务体系，旨在通过完善的数字证书和密钥管理，为用户提供透明且安全的加解密和数字签名服务
- 公钥基础设施包括：
  - 认证授权(Certificate Authority, CA)中心
  - 注册授权(Registration Authority, RA)中心
  - 策略管理
  - 数字证书和密钥管理
  - 密钥的备份与恢复

知识讲解



公钥基础设施

- 数字证书是公钥密码体系中的权威电子文档，也是网络环境中的身份证，用来证明一个主体(用户、服务器等)的身份及其私钥合法性的数字ID
- 基于公钥基础设施的应用有很多：
  - 安全Web服务器
  - 安全电子邮件
  - 电子数据交换
  - 互联网环境中的电子支付、信用卡交易等

知识讲解

信息隐藏技术

知识讲解

- 不同于将明文编码为密文的加解密技术，信息隐藏技术是利用人类感觉器官对数字信号的感觉冗余，将一些秘密信息以伪装的方式隐藏在非秘密信息之中，达到在网络环境中隐蔽通信和标识的目的
- 信息隐藏技术由两部分组成：
  - 信息嵌入
  - 信息提取
- 目前信息隐藏技术的典型应用包括：
  - 隐蔽信道
  - 匿名通信
  - 数字水印
  - 隐写术等

应用技术

IP安全

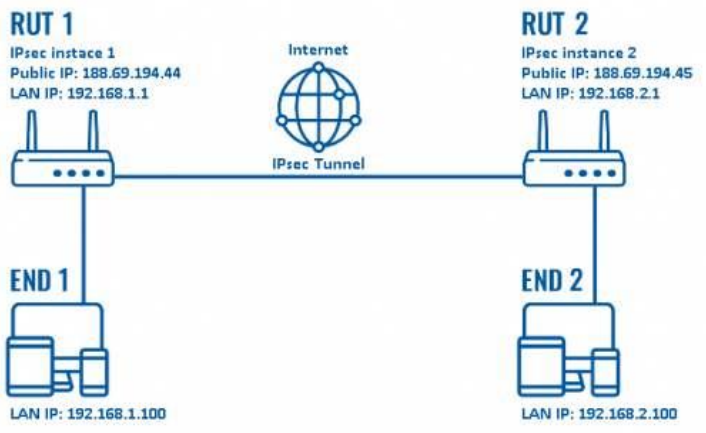
- IP协议本身是不安全的，IP分组的头部很容易伪造，而其内容同样易被读取和写入。数据报文的接收方通常很难确认该报文真的来自其所声称的源地址，也无法确信其内容在传输过程中未遭窥探和篡改
- 互联网工程任务组(Internet Engineering Task Force, IETF)于1995年成立了一个专门研究为IP协议引入密钥管理机制的组织，该组织提出了一系列在IP协议的基础上，保证数据传输安全的标准，称为IP安全协议(IP Security Protocol, IPSec)，该协议是IPv6的一部分，可以为IPv4和IPv6提供互操作、高质量和基于密码的安全性

知识讲解

IP安全

- IP安全协议提供的安全服务包括：
  - 访问控制
  - 数据完整性验证
  - 数据源认证
- IP安全协议并非单一协议，而是一个协议族，具体包括：
  - 认证头协议
  - 封装安全载荷协议
  - 互联网安全关联密钥管理协议
  - 密钥交换协议
  - 加密与认证算法

知识讲解



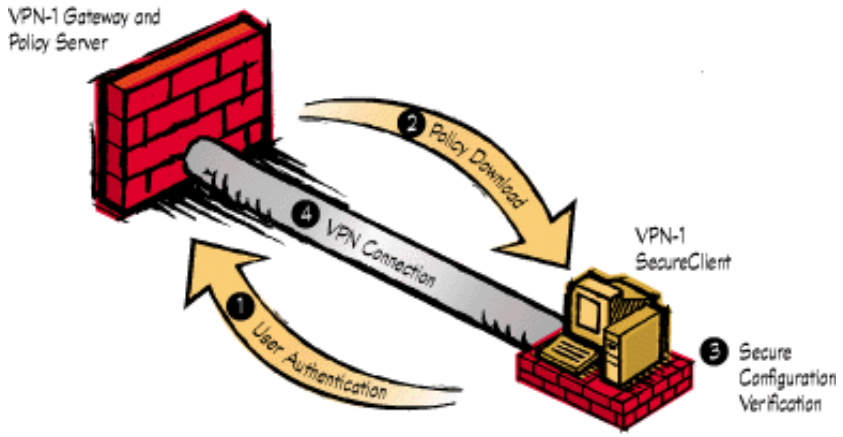
虚拟专用网络技术

- 虚拟专用网络(Virtual Private Network, VPN)是指在公用网络之上借助加密通信建立起来的专用网络
- 虚拟专用网络属于远程访问技术。所谓远程访问是指从局域网外部对局域网内部的服务器资源所进行的访问
- 在传统企业网配置中，要进行远程访问，有两种方案可供选择：
  - 租用数字数据网(Digital Data Network, DDN)专线或帧中继，但这样做的通信和维护费用十分昂贵
  - 较廉价的方案是通过互联网进入企业内网，但这样做又势必带来极大的安全隐患

知识讲解

虚拟专用网络技术

- 基于虚拟专用网络的远程访问：
  - 远程用户通过互联网连接企业的虚拟专用网络服务器，再通过该服务器进入企业内网，虚拟专用网络服务器和远程客户端之间以加密方式传输数据
  - 由于采用了加密通信，可以认为数据在一条安全的通信隧道里传输，如同专门架设了一个专用网络，谓之虚拟专用网络
- 虚拟专用网络所涉及到的关键技术包括：
  - 隧道技术
  - 密码技术
  - 密钥管理技术
  - 用户和设备认证技术



知识讲解

电子邮件安全技术

- 电子邮件的安全隐患及对策：
  - 以明文形式传输的邮件内容很容易被截获
    - 借助对称密码体系，对邮件做内容加密
  - 邮件的接收者无法确信邮件的发送者是谁
    - 借助公钥密码体系，对邮件做数字签名
- 电子邮件安全技术包括：
  - 端到端安全电子邮件技术
  - 传输层安全电子邮件技术
  - 电子邮件服务器安全技术

知识讲解

Web安全技术

- 根据攻击对象的不同，可将Web攻击分为：
  - Web服务器攻击
  - Web浏览器攻击
  - Web通信信道攻击
- 根据攻击性质的不同，可将Web攻击分为：
  - 主动型Web攻击
  - 被动型Web攻击
- 根据攻击目标的不同，可将Web攻击分为：
  - 数据完整性和保密性Web攻击
  - 认证鉴别和拒绝服务Web攻击

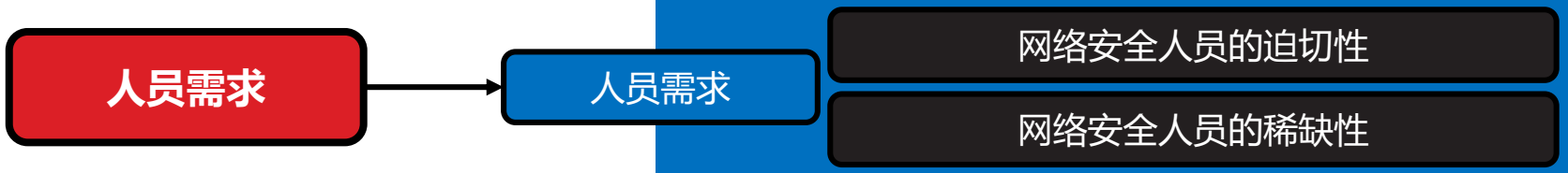
知识讲解

Web安全技术

- Web的安全漏洞多种多样：
  - 被植入恶意代码的CGI程序能够自由地访问系统资源，令系统失效，删除文件，盗取用户资料，控制服务器
  - 动态页面中嵌入的恶意代码在用户浏览网页的同时被自动下载运行，窃取用户信息或对用户系统造成破坏
  - 能够从互联网上下载的应用软件和工具程序名目繁多，用户完全无从分辨哪些是可信的，哪些是有害的
- Web安全技术分别从网络层、传输层和应用层着手，通过操作系统、数据库、防火墙、应用程序等多种手段，为用户营造可信且安全的互联网环境

知识讲解

人员需求



人员需求

网络安全人员的迫切性

- 我们处在风险之中，计算机控制了供电、通信、航空和金融服务，它们被用来存储至关重要的信息
- 尽管我们信任计算机，但它们具有易于受到事故破坏和故意攻击的缺陷，这也是最值得人们警惕的
- 现代窃贼用计算机比用枪支能够偷到更多的东西，也许明天的恐怖分子能够用键盘比用炸弹造成更大的破坏
- 重中之重是人员的培训，在一切基础设施的建设中，最紧迫，最困难，也是其它一切因素的先决条件，是建立一支训练有素的信息安全专家队伍
- 我国互联网用户数量位居世界第一，各种网络应用和业务模式蓬勃发展，急需加强网络安全专业人才的培养

知识讲解

网络安全人员的稀缺性

- 社会急需大量、各个层次的网络安全技术人才
- 高层次网络安全人才培养是相当重要和艰巨的任务
- 涉及我国网络安全的核心技术必须由我国的技术专家掌握

知识讲解

课程简介


课程简介
课程简介
网络安全概述
网络协议栈
对称密钥
公钥密码
消息摘要
嗅探器
安全Web服务器
端口扫描
网络诱骗
入侵检测
防火墙
内核加固

课程简介

网络安全概述

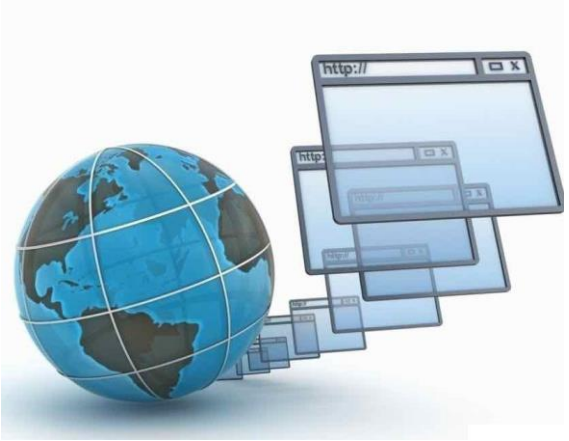
- 本单元旨在帮助学生建立起网络安全的基本概念，了解目前阶段来自网络威胁的主要挑战，网络安全学科所涉及到的技术门类和专业范围，网络安全领域对从业者的技术要求，最后是对整个课程体系的概要性介绍

知识讲解

网络协议栈

- Linux作为应用最广泛的开源操作系统之一，不仅能够提供终端主机所需要的各种网络协议软件，而且还能够实现网桥、路由器等网络设备的基本功能
- 为了帮助学生获得自主知识产权网络安全软件产品的研发能力，本课程所有案例均在Linux操作系统上完成
- 本单元将从两个方面对Linux网络协议栈展开讨论，一是结合Linux网络协议栈的设计特点，介绍网络协议栈源码的几个主要功能模块，二是讨论Linux网络协议栈源码发送和接收TCP报文的基本流程

知识讲解



对称密钥

- DES算法是一种典型的对称密钥加密算法，也是应用密码学中最基本的加密算法之一，目前广泛应用于网络通信加密、数据存储加密、口令与访问控制系统之中
- 掌握DES算法在网络通信中的应用对于理解对称加密算法大有裨益
- 本单元以加密TCP聊天程序为案例，研究基于DES算法的通信加密应用软件的设计和编程方法
- 本单元旨在帮助学生理解对称加密算法DES的基本工作原理，掌握将DES算法应用于网络通信的设计与软件编程的基本方法，掌握Linux操作系统socket编程的基本方法
- 通过本单元的学习，学生应能利用socket编写一个TCP聊天程序，其聊天内容在传输过程中通过DES算法加密和解密

知识讲解

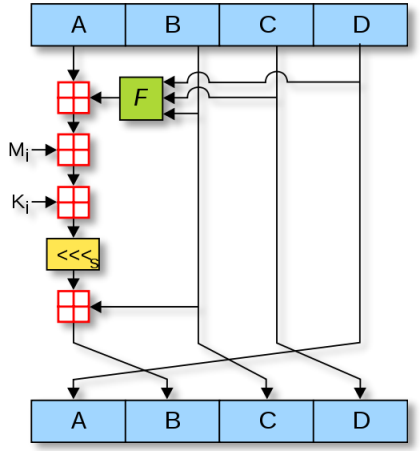
公钥密码

- 在讨论了对称加密算法DES的原理与实现的基础上，本单元以典型的非对称加密算法RSA为例，以进一步完善加密TCP聊天程序为目标，系统地讨论公钥密码体系与RSA算法的基本工作原理和应用软件编程方法
- 本单元旨在帮助学生理解非对称加密算法RSA的基本工作原理，掌握将RSA算法应用于网络通信的设计与软件编程的基本方法，了解在Linux操作系统上实现异步I/O的基本方法
- 通过本单元的学习，学生应能在上一单元加密聊天程序的基础上，增加基于RSA算法的密钥分发功能，用公私钥对DES密钥加解密

知识讲解

消息摘要

- MD5是目前最流行的消息摘要算法，已被广泛应用于数字签名、文件完整性检测等领域
- 熟悉MD5算法对于开发安全的网络应用程序具有重要的意义
- 本单元旨在帮助学生理解MD5消息摘要算法的基本原理，掌握利用MD5算法生成消息摘要的计算方法，掌握将MD5算法应用于文件完整性校验软件的基本设计与编程方法，掌握在Linux操作系统中检查文件完整性的基本方法
- 通过本单元的学习，学生应能正确实现MD5摘要的计算过程，对任意长度的字符串和文件能够生成128位长的MD5摘要，并通过该摘要验证文件的完整性



知识讲解

嗅探器

- 网络监控软件能够监测网络流量，发现网络中异常的数据流，有效地发现和防御网络攻击，是保证网络安全的重要工具和手段之一，也是网络安全技术人员必须掌握的重要技能之一
- 本单元研究基于原始套接字(Raw Socket)的网络嗅探器(Sniffer)系统的设计和软件编程方法
- 本单元旨在帮助学生理解Sniffer的基本工作原理和实现方法，掌握Raw Socket的基本工作原理，掌握TCP/IP、ICMP等协议及socket编程方法
- 通过本单元的学习，学生应能利用原始套接字编写一个网络嗅探器捕获网络数据包，分析基本的数据包信息并实现简单的过滤器功能

知识讲解

安全Web服务器

- Web服务使用HTTP协议传输明文，重要数据有被第三方截获的风险。安全超文本传输协议(HTTP over SSL，HTTPS)通过安全套接字层(Secure Socket Layer，SSL)加密HTTP数据，保护数据在Web系统中的传输安全
- 掌握基于OpenSSL的安全Web服务器软件的设计和编程方法，对于提高Web系统的安全性有着重要的意义
- 本单元旨在帮助学生理解HTTPS协议和SSL协议的基本工作原理，掌握使用OpenSSL库编程的方法，掌握安全Web服务器的基本设计与实现方法
- 通过本单元的学习，学生应能在Linux平台上基于OpenSSL库，编写一个安全Web服务器程序，该服务器能并发处理多个请求，至少支持HTTPS协议下最基本的GET命令，进而扩展到支持HEAD、POST以及DELETE等命令，编写必要的客户端程序，以发送HTTPS请求，并显示服务器返回的响应结果

知识讲解

端口扫描

- 网络端口扫描器不仅可以发现目标主机的开放端口和操作系统类型，还可以获知系统的安全漏洞和口令缺陷，既是重要的网络检测设备，同时也是黑客的攻击工具
- 掌握端口扫描器的基本工作原理和软件设计方法是对网络安全技术人员的起码要求，对维护网络安全，了解黑客攻击手段有着重要的意义
- 本单元旨在帮助学生理解网络端口扫描器的基本结构、工作原理和设计方法，掌握TCP CONNECT扫描、TCP SYN扫描、TCP FIN扫描以及UDP扫描的基本工作原理、设计与实现方法，掌握ping程序的设计与实现方法，掌握Linux操作系统多线程编程的基本方法
- 通过本单元的学习，学生应能编写端口扫描程序，实现TCP CONNECT扫描、TCP SYN扫描、TCP FIN扫描和UDP扫描等四种基本扫描方式，设计并实现ping程序，探测目标主机是否可达

知识讲解

网络诱骗

- 网络诱骗系统通常会通过一些诱饵来诱惑潜在的攻击者发起攻击，同时对其攻击行为进行监控和记录，评估其危害，搜集犯罪证据，以达到主动保护系统安全的目的
- 网络诱骗系统的主要技术包括伪装技术、监控技术和隐藏技术
- 本单元旨在帮助学生理解网络诱骗系统的基本工作原理，理解Linux系统调用的原理和实现，以及利用钩子技术扩展操作系统自带编程接口的方法，掌握可加载内核模块编程的相关知识和方法，了解Linux系统中程序隐藏的方法
- 通过本单元的学习，学生应能设计并实现一个简单的网络诱骗系统，该系统运行在Linux操作系统的核心层(Ring 0)，将用户终端登录后的键盘输入记录在日志文件中，甚至可以尝试为该系统添加隐藏(模块、文件、通信等)功能

知识讲解

入侵检测

- 入侵检测系统(IDS)是一种对网络传输进行实时监测，并在发现可疑情况时发出警报或采取主动防御措施的网络安全设备
- 本单元在系统分析入侵检测系统基本工作原理的基础上，以基于特征的入侵检测系统为案例，研究入侵检测系统的设计与软件编程方法
- 本单元旨在帮助学生掌握基于特征的入侵检测系统的基本工作原理、设计和实现方法，掌握K-Means聚类算法的计算过程，掌握在网络安全系统中应用数据挖掘技术的基本概念和方法
- 通过本单元的学习，学生应能使用KDD Cup 1999数据集进行聚类分析，训练一个用于入侵检测的聚类模型，并使用该模型对测试数据进行预测

知识讲解

防火墙

- 防火墙通过在网络与网络或网络与主机之间建立访问控制以及地址隐藏等技术手段，保护网络资源免受非法侵害，是目前常用的网络安全设备之一
- Linux系统通过Netfilter内核模块提供了包过滤功能，可以此作为构建防火墙的基础
- 本单元通过扩展Netfilter内核模块实现防火墙的功能，同时也讨论了通过IPTables快速搭建自定义防火墙的方法
- 本单元旨在帮助学生理解防火墙技术的基本工作原理，理解Linux环境中Netfilter/IPTables的工作机制，掌握对Netfilter内核模块进行扩展编程的基本方法，掌握通过IPTables构建防火墙的基本方法
- 通过本单元的学习，学生应能通过扩展Netfilter内核模块的方法实现简单的防火墙，以基于协议、源IP地址或目的端口号的方式过滤数据包

知识讲解

内核加固

- Linux是一种开源操作系统，开发人员可以通过修改其源代码对系统进行加固
- 本单元通过加固Linux网络协议栈程序，改变Linux内核对孤立TCP SYN数据包的处理方式，提升系统对TCP SYN拒绝服务攻击的防御能力
- 本单元旨在帮助学生理解TCP连接的建立过程以及拒绝服务攻击的基本原理和方法，通过分析Linux内核源码，理解Linux网络协议栈的实现原理，掌握对TCP SYN洪泛的防御手段以及对Linux内核进行扩展开发的方法，了解Linux TCP Cookie防火墙的工作原理
- 通过本单元的学习，学生应能通过扩展Linux原有的内核功能，使其在遭受TCP SYN拒绝服务攻击时，主动丢弃TCP SYN数据包，在不影响已建立TCP连接的前提下，提高系统抵御拒绝服务攻击的能力

知识讲解

总结和答疑