(2020秋季 课程编号：COMP6216P)

网络安全
第1章 概述

曾凡平

billzeng@ustc.edu.cn

联系方式及资源地址

老师主页：**http://staff.ustc.edu.cn/~billzeng/**

电子邮件：**billzeng@ustc.edu.cn**

辅导老师：

申敬飞 ericjeff@mail.ustc.edu.cn

张伟康 buttman@mail.ustc.edu.cn

课程资源：

① 研究生信息平台的教学信息

② **http://cybersecurity.ustc.edu.cn/**

课程教学大纲

- 本课程从**网络攻防**的角度，以**专题**的形式详细介绍**网络信息安全**的基本原理和技术。

- 主要内容包括：网络攻防概述、密码学及其应用、虚拟专用网（IPsec）、防火墙、入侵检测、网络入侵、拒绝服务攻击、恶意代码攻击，以及其他信息安全技术等内容。

- 本课程旨在提高学员的网络安全防护意识；通过网络攻防实践，增强网络信息安全的**实践能力**。

课程简介

- 专业课：60学时理论+自修实验
- **教室：未来中心3号报告厅 :6(6,7,8) 曾凡平**
  - **第6小节：14:00-14:45**
  - **第7小节：14:50-15:35**
  - **第8小节：15:40-16:25**
- 教学对象：
  - 对网络攻防(**理论与技术**)知之不多，想对网络信息安全有所了解，试图提高网络与信息系统安全**实践能力**的同学。
- 成绩评定方式：
  - 作业30%+实验报告20%
  - 期末考试或课程报告50%
- 作业写在作业本上，手机拍照转换成PDF文档**提交到研究生信息平台，一周内完成**；实验报告用A4排版，转换成PDF文档**提交到研究生信息平台，二周内完成**。

课程主要内容

- 网络攻防三大关键技术
  - **①网络侦察：获取目标信息**
  - **②网络攻击：抑制、入侵、控制**
  - **③网络防护：防止被攻击**

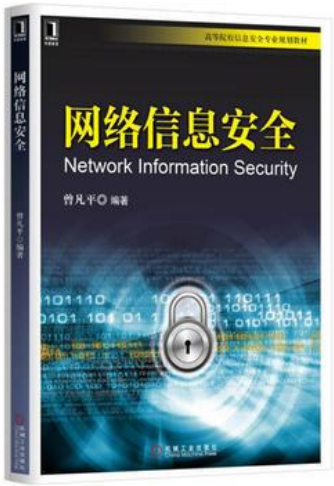
➢ **漏洞(vulnerability)分析与利用是核心**

- 缓冲区溢出漏洞的利用(调试工具的使用)

教材及授课方式

- 教材
  - 《网络信息安全》
  - 曾凡平编著，机械工业出版社,
  - 2019年8月第1版第5次印刷
- 主要参考书
  - 《黑客大曝光》序列从书: **(攻击)**
  - 《网络安全概论》: **(防护)**

    刘建伟，毛剑，胡荣磊，电子工业出版社，2009



- 授课方式：多媒体教学 + **演示实验** + **实验报告**

第1讲 网络安全概述

1.1 网络安全概述	• 1.1.1 网络安全概念 • 1.1.2 网络安全体系结构 • 1.1.3 网络安全的攻防体系
1.2 计算机网络面临的安全威胁	• 1.2.1 TCP/IP网络体系结构及计算机网络的脆弱性 • 1.2.2 计算机网络面临的主要威胁
1.3 计算机网络安全的主要技术与分类	• 1.3.1网络侦察 • 1.3.2网络攻击 • 1.3.3网络安全防护
1.4 网络安全的起源与发展	• 1.4.1 计算机网络的发展 • 1.4.2 网络安全技术的发展 • 1.4.3 黑客与网络安全

1.1 网络安全概述

1.1.1 网络安全概念

- **网络安全(network security)是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。**
- 网络安全大体上可以分为**信息系统**（如主机、网络服务器）的安全、**网络边界**的安全及**网络通信**的安全。
- 网络安全的目标是**保护**网络系统中信息的机密性、完整性、可用性、不可抵赖性和可控性等**安全属性**。机密性、完整性、可用性也称为信息安全的**三要素**。

信息安全的三要素

- **机密性Confidentiality**
  - **机密性（保密性）**是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。
  - 它的任务是确保信息不会被未授权的用户访问。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。

信息安全的三要素之：完整性Integrity

- **完整性是指维护信息的一致性**，即信息在生成、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。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。
- 信息的完整性包括两个方面：

  (1) **数据完整性**：数据没有被(未授权)篡改或者损坏；

  (2) **系统完整性**：系统未被非法操纵，按既定的目标运行。

信息安全的三要素之：可用性Availability

- 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。

不可抵赖性、真实性、可控性和可审查性

- **不可抵赖性**
  - 不可抵赖性是信息交互过程中，所有参与者不能否认曾经完成的操作或承诺的特性。
- **真实性**
  - 信息的真实性要求信息中所涉及的事务是客观存在的，信息的各个要素都真实且齐全，信息的来源是真实可靠的。
- **可控性**
  - 信息的可控性是指对信息的传播及内容具有控制能力。也就是可以控制用户的信息流向，对信息内容进行审查，对出现的安全问题提供调查和追踪手段。
- **可审查性**
  - 出现安全问题时提供依据与手段，它以可控性为基础。
- **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。

四大安全属性？

- 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：

A. 机密性

B. 可认证性：
   - 通过哈希函数实现信息的可认证？

C. 不可抵赖

D. 完整性

1.1.2 网络安全体系结构

- 网络安全体系结构是**安全服务、安全机制、安全策略及相关技术**的集合。
- 国际标准化组织(ISO)于1988年发布了ISO 7498-2标准，即开放系统互联(OSI， Open System Interconnection)安全体系结构标准，该标准等同于中华人民共和国国家标准的GB/T 9387.2-1995。
- 1990年，国际电信联盟(ITU，International Telecommunication Union)决定采用ISO 7498-2作为其X.800推荐标准。因此，X.800和ISO 7498-2标准基本相同。
- 1998年，RFC 2401(Last updated 2013-03-02)给出了Internet协议的安全结构，定义了IPsec适应系统的基本结构，这一结构的目的是为IP层传输提供多种安全服务。
- 2005年RFC 4301(Last updated 2020-01-21)更新了RFC 2401。

与安全体系结构相关的术语

(1) 安全服务

- X.800对安全服务做出定义：为了保证系统或数据传输有足够的安全性，开放系统通信协议所提供的服务。
- RFC 2828也对安全服务做出了更加明确的定义：安全服务是一种由系统提供的**对资源进行特殊保护的进程或通信服务**。

(2) 安全机制

- 安全机制是一种**措施或技术**，一些软件或实施一个或更多安全服务的**过程**。
- 常用的安全机制有认证机制、访问控制机制、加密机制、数据完整性机制、审计机制等。

与安全体系结构相关的术语

(3) 安全策略

- 所谓安全策略，是指在某个安全域内，施加给所有与安全相关活动的**一套规则**。所谓安全域，通常是指属于某个组织机构的一系列处理进程和通信资源。这些规则由该安全域中所设立的安全权威机构制定，并由安全控制机构来描述、实施或实现。

(4) 安全技术

- 安全技术是与安全服务和安全机制对应的一序列**算法、方法或方案**，体现在相应的软件或管理规范等之中。比如密码技术、数字签名技术、防火墙技术、入侵检测技术、防病毒技术和访问控制技术等。

图1.1 分层的网络安全体系结构

应用层	应用层安全协议，如：HTTPS、SSH、FTPS
传输层	传输层安全协议，如：SSL、TLS
网络层	网络层安全协议，如：IPSec
网络接口层	网络接口层安全技术，如：PPTP、L2TP

1.1.3 网络安全的攻防体系

- **网络攻击**是指采用技术手段，利用目标信息系统的安全缺陷，破坏网络信息系统的保密性、完整性、真实性、可用性、可控性与可审查性等的措施和行为。其目的是窃取、修改、伪造或破坏信息，以及降低、破坏网络使用效能。

- **网络防护**是指为保护己方网络和设备正常工作、信息数据安全而采取的措施和行动。其目的是保证己方网络数据的保密性、完整性、真实性、可用性、可控性与可审查性等。

1.2 计算机网络的脆弱性及面临的安全威胁

层和协议的集合称为网络体系结构 (network architecture)

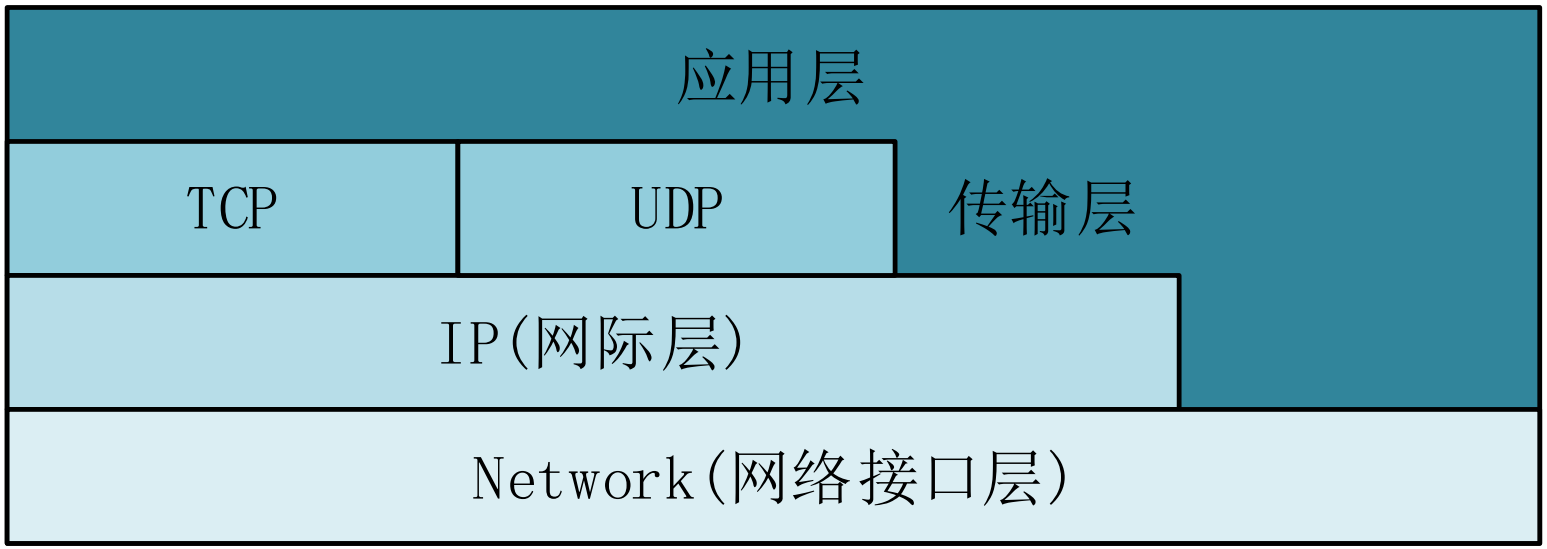


图1.2 TCP/IP网络体系结构

1.2.1 TCP/IP网络体系结构及计算机网络的脆弱性

(1) 网络基础协议存在安全漏洞

- TCP/IP协议在设计的初期并没有考虑安全性，从而导致大量的安全问题。如：地址欺骗、源路由攻击

(2) 网络硬件存在着安全隐患

- 计算机硬件在制造和使用的过程中会存在一些安全隐患。
- 故意放置漏洞、技术原因、环境的影响

(3) 软件缺陷和安全漏洞

- 软件是网络信息系统的核心。然而由于技术或人为因素，软件不可避免地还存在缺陷，这就可能导致安全漏洞的出现。
- 对程序输入的处理不当；缺乏适当的用户身份认证；对程序功能的配置处理不当

(4) 操作系统存在安全隐患

- 首先，操作系统也是软件系统，而且是巨型复杂高纬度的软件，其代码量非常庞大，由成百上千工程师协作完成，很难避免产生安全漏洞。
- 其次，操作系统的功能越来越多，配置起来越来越复杂，从而会造成配置上的失误，产生安全问题。
- 再次，操作系统的安全级别不高。目前大规模使用的Windows和Linux系统的安全级别为TCSEC的C2级，而C2级难以保证信息系统的安全。
- 此外，我国目前特别严重的问题是**操作系统基本上自国外引进**，不能排除某些国家出于不可告人的目的而在其中设置了后门，一旦发生国家之间的冲突，则后果不堪设想。因此，软件（特别是操作系统）国产化是一个迫切需要解决的根本问题。

(5) 网络体系结构的安全风险

- 进行网络体系结构设计时，是否按安全体系结构和安全机制进行设计，直接关系到网络平台的安全性能。

- 网段划分是否合理，路由是否正确，网络的容量、带宽是否考虑客户上网的峰值，网络设备有无冗余设计等都与安全风险密切相关。

- 对于目前的网络，其体系结构异常复杂，除了要考虑传统的安全问题，还要考虑跨域的安全问题。

1.2.2 计算机网络面临的主要威胁

- 计算机网络面临的安全威胁形形色色：有人为和非人为的、恶意的和非恶意的、内部攻击和外部攻击等。

- 对网络安全的威胁主要表现在：非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等方面。

- **安全威胁主要利用网络与信息系统存在的脆弱性和网络管理中的漏洞。**

网络面临的主要威胁

(1) 各种自然因素

- 包括各种自然灾害；电磁辐射和电磁干扰的威胁；网络硬件设备自然老化，可靠性下降等。

(2) 内部窃密和破坏

- 内部涉密人员有意或无意泄密、更改记录信息；内部非授权人员有意无意偷窃机密信息、更改网络配置和记录信息；内部人员破坏网络系统。

(3) 信息的截获和重演

- 通过搭线等方式，截获机密信息，或通过对信息流和流向、通信频度和长度等参数的分析，推出有用信息。它不破坏传输信息的内容，不易被查觉。截获并录制信息后，可以在必要的时候重发或反复发送这些信息。

网络面临的主要威胁

(4) 非法访问

- 非法访问指的是未经授权使用网络资源或以未授权的方式使用网络资源，它包括：非法用户（如黑客）进入网络或系统，进行违法操作；合法用户以未授权的方式进行操作。

(5) 破坏信息的完整性

- 攻击可能从三个方面破坏信息的完整性：改变信息流的时序，更改信息的内容；删除某个消息或消息的某些部分；在消息中插入一些信息，让收方读不懂或接收错误的信息。

(6) 欺骗

- 攻击者可能冒充合法地址或身份欺骗网络中的其它主机及用户；冒充网络控制程序套取或修改权限、口令、密钥等信息，越权使用网络设备和资源；接管合法用户，欺骗系统，占用合法用户的资源。

网络面临的主要威胁

(7) 抵赖

- 可能出现下列抵赖行为：发信者事后否认曾经发送过某条消息；发信者事后否认曾经发送过某条消息的内容；发信者事后否认曾经接收过某条消息；发信者事后否认曾经接收过某条消息的内容。

(8) 破坏系统的可用性

- 攻击者可能从下列几个方面破坏网络系统的可用性：使合法用户不能正常访问网络资源；使有严格时间要求的服务不能及时得到响应；摧毁系统。

1.3 计算机网络安全的主要技术与分类

- 从系统的角度可以把网络安全的研究内容分成三类：
  - 网络侦察（信息探测）
  - 网络攻击
  - 网络防护

- 网络安全的主要技术也可以相应的划分为三类
  - 网络侦察技术
  - 网络攻击技术
  - 网络防护技术

1.3.1 网络侦察

- 也称为网络信息探测，是指运用**各种技术手段**、采用适当的策略对目标网络进行探测扫描，获得有关目标计算机网络系统的拓扑结构、通信体制、加密方式、网络协议与操作系统、系统功能，以及目标地理位置等各方面的有用信息，并进一步判别其主控节点和脆弱节点，**为实施网络攻击提供可靠的情报保障**。

(1) 端口探测技术

- 主要利用端口扫描技术，以发现网络上的活跃主机及其上开放的协议端口。一般利用端口扫描软件进行端口探测，如开源软件**nmap**就提供了丰富的端口探测功能。

网络侦察

(2) 漏洞探测技术

- 在硬件、软件、协议的具体实现或系统安全策略上不可避免会存在缺陷。**如果这些缺陷能被攻击者利用，则这样的缺陷称为漏洞。**
- 漏洞探测也称为漏洞扫描，是指利用技术手段，以获得目标系统中漏洞的详细信息。
- 目前有两种常用的漏洞探测方法。
  - **① 模拟攻击**
  - **② 信息型漏洞探测**

网络侦察

(3) 隐蔽侦察技术

- 一般来说，重要的信息系统都具有很强的安全防护能力和反侦察措施，常规侦察技术很容易被目标主机觉察或被目标网络中的入侵检测系统发现，因而要采用一些手段进行隐蔽侦察。隐蔽侦察采用的主要手段有：秘密端口探测、随机端口探测、慢速探测等。

(4) 渗透侦察技术

- 渗透侦察指的是在目标系统中植入特定的软件，从而完成情报的收集。渗透侦察技术主要采用反弹端口型木马技术。
- 为了将木马植入到目标系统中，一般采用诱骗方法使目标用户主动下载木马软件。

1.3.2 网络攻击

- 计算机网络攻击是指利用目标计算机网络系统的安全缺陷（漏洞），为窃取、修改、伪造或破坏信息，以及降低、破坏网络使用效能而采取的各种措施和行动。

- 其目的是破坏网络信息系统的安全属性。

- 由于计算机硬件和软件，网络协议和结构，以及网络管理等方面不可避免地存在安全漏洞，使得网络攻击成为可能。

网络攻击技术

(1) 拒绝服务攻击

- **拒绝服务（Denial of Service, DoS）**攻击的主要目的是降低或剥夺目标系统的可用性，使合法用户得不到服务或不能及时得到服务，一般通过耗尽网络带宽或耗尽目标主机资源的方式进行。

(2) 入侵攻击

- 入侵攻击是指攻击者利用目标系统的漏洞非法进入系统，以获得一定的权限，进而可以窃取信息、删除文件、埋设后门、甚至瘫痪目标系统等行为。

(3) 病毒攻击

- 计算机病毒一般指同时具有感染性和寄身性的代码。它隐藏在目标系统中，能够自我复制、传播和侵入到其它程序中去，并篡改正常运行的程序，损害这些程序的有效功能。

(4) 恶意代码攻击

- 恶意代码是指任何可以在计算机之间和网络之间传播的程序或可执行代码，其目的是在未授权的情况下有目的地更改或控制计算机及网络系统。计算机病毒就是一种典型的恶意代码，此外，还包括木马、后门、逻辑炸弹、蠕虫等。

(5) 电子邮件攻击

- 利用电子邮件缺陷进行的攻击称为电子邮件攻击。
- 传统的邮件攻击主要是向目标邮件服务器发送大量的垃圾邮件；现在的邮件攻击更多地是发送伪造或诱骗的电子邮件，诱骗用户去执行一些危害网络安全的操作。

(6) 诱饵攻击

- 诱饵攻击指通过建立诱饵网站，诱骗用户去浏览恶意网页，从而实现攻击。诱饵攻击是一种被动攻击，只要用户保持足够的警觉就可以避免。

1.3.3 网络安全防护

- **计算机网络防护是指为保护己方网络和设备正常工作，保护信息数据安全而采取的措施和行动。**
- 其目的是保护网络信息系统的安全属性

- 网络攻击和网络防护是矛和盾的关系。在建立网络安全防护体系时，**必须走管理和技术相结合的道路**。
- 网络安全防护的涉及面很宽，从技术层面上讲主要包括防火墙技术、入侵检测技术、病毒防护技术、数据加密技术和认证技术等。
- 网络安全防护的主要目标可以归结为“五不”：**进不来、拿不走、看不懂、改不了、走不掉。**

网络安全防护的5个主要目标

1)“**进不来**”：**使用访问控制机制**，阻止非授权用户进入网络，从而保证网络系统的**可用性**；

2)“**拿不走**”：**使用授权机制**，实现对用户的权限控制，同时结合内容审计机制，实现对网络资源及信息的**可控性**；

3)“**看不懂**”：**使用加密机制**，确保信息不暴露给未授权的实体或进程，从而实现信息的**保密性**；

网络安全防护的5个主要目标

4)“改不了”：使用**数据完整性鉴别**机制，保证只有得到允许的人才能修改数据，从而确保信息的**完整性和真实性**；

5)“走不掉”：使用**审计、监控、防抵赖**等安全机制，使得破坏者走不脱。并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

(1) 防火墙技术

- **防火墙是实现网络访问控制的装置**，是最基本的网络防护措施，也是目前使用最广泛的一种网络安全防护技术。
- 防火墙通常安置在内部网络和外部网络之间，以抵挡外部入侵和防止内部信息泄密。防火墙是一种综合性的技术，涉及到计算机网络技术、密码技术、安全协议、安全操作系统等多方面。防火墙的主要作用为过滤进出网络的数据包、管理进出网络的访问行为、封堵某些禁止的访问行为、记录通过防火墙的信息内容和活动、对网络攻击进行检测和告警等。
- 简单的防火墙可以用路由器实现，复杂的可以用主机甚至一个子网来实现。防火墙技术主要有两种：**数据包过滤技术和代理服务技术**。

(2)入侵检测技术

- 入侵检测是一种**动态安全技术**，通过对入侵行为的过程与特征的研究，使安全系统对入侵事件和入侵过程能做出实时响应。

- 有两种主要的入侵检测技术：基于**特征**的检测和基于**行为**的检测，也称为**误用检测**和**异常检测**。

- 入侵检测系统从实现方式上一般分为两种，即**基于主机**的入侵检测系统和**基于网络**的入侵检测系统。

(3)计算机病毒及恶意代码防治技术

- 计算机病毒的检测就是要自动地发现或判断文件、内存以及网络中传输的信息是否含有病毒。检测病毒的主要方法是**特征码及行为分析法**。
- **特征码是某种病毒或恶意代码的唯一特征**，如果某些代码具有病毒的特征就可以判定为病毒。对于变形病毒，每传播一次其特征就会改变，基于特征码的检测方法将失效，这时就要利用行为分析法。
- **行为分析法**通过判断代码**是否有破坏信息系统的行为**，从而判定是否为病毒。例如，如果某段代码修改可执行文件、修改库文件、修改文档中的宏(可执行的脚本)等，则很可能是病毒。

(4) 密码技术

- 密码技术主要研究数据的**加密和解密**及其应用。密码技术是确保计算机网络安全重要机制，是信息安全的基石。密码技术有两种体制：单密钥体制和双密钥体制。
- **单密钥体制**也称为**传统密码体制**，其加密密钥和解密密钥相同，或解密密钥和加密密钥可以相互推断出来。DES、IDEA以及AES都是典型的单密钥体制的密码算法。这类算法的运行速度快，适合对大量数据的加/解密。
- **双密钥体制**也称为**公开密钥加密体制**，需要一对密钥，即公钥和私钥。公钥用于加密，私钥用于解密。如RSA算法。公钥算法的运行速度较慢，适合对少量数据的加/解密，主要用于**密钥分配和数字签名**。

认证技术和蜜罐技术

(5) 认证技术

- 认证主要包括**身份认证**和**信息认证**。身份认证是验证信息的发送者的真实身份；信息认证验证信息的完整性，即验证信息在传送或存储过料中是否被窜改，重放或延迟等。

(6) “蜜罐”技术

- “蜜罐”是试图将攻击者从关键系统引诱开的**诱骗系统**。也就是在内部系统中设立一些陷阱，用一些主机去模拟一些业务主机甚至模拟一个业务网络，给入侵者造成假象。

1.4 网络安全的起源与发展

- 网络安全的发展是与计算机及网络技术的发展分不开的。
- 此外，安全防护技术也随黑客攻击技术的发展而发展。

1.4.1 计算机网络的发展

- 1950年代中后期，许多系统都将地理上分散的多个终端通过通信线路连接到一台中心计算机上，这样就出现**以单台计算机为中心的远程联机系统**。

- 在主机前设置一个通信控制处理机和线路集中器。这种**多机系统也称为复杂的联机系统**，出现于1960年代-计算机网络的雏形。
-
- **初期的计算机网络以多个主机通过通信线路互联起来，为用户提供服务，兴起于1960年代后期**，典型代表是美国国防部高级研究计划局协助开发的**ARPAnet**。

计算机网络的发展

- 1970年代以来，特别是Internet的诞生及广泛应用，使得计算机网络得到了迅猛的发展。
- **1982年**，Internet由ARPAnet、MILnet等几个计算机网络合并而成，作为Internet的早期主干网。
- **到了1986年**，又加进了美国国家科学基金会的NSFnet、美国能源部的ESnet、国家宇航局的NSI，这些网络把美国东西海岸相互连接起来，形成美国国内的主干网。
- 1988年，**作为学术研究使用的**NFSnet**开始对一般研究者开放**。
- **1994年**，连接到Internet上的主机数量达到了320万台，连接世界上的3万多个计算机网络。从此以后计算机网络得到了飞速的发展并在世界范围内得到广泛的应用。

第45次《中国互联网络发展状况统计报告》

- 4月28日，中国互联网络信息中心（CNNIC）发布第45次《中国互联网络发展状况统计报告》（以下简称:《报告》）。
- 《报告》从六个方面综合反映2019年及2020年初我国互联网发展状况：

① 网民规模突破9亿，为数字经济发展打下坚实用户基础

② 疫情期间部分互联网应用呈现快速增长态势

③ 在线教育呈现爆发式增长

④ 全国一体化政务服务平台在疫情防控中发挥有力支撑

⑤ 抗击疫情加速互联网产业发展 带来新机遇与挑战

⑥ 我国技术创新能力持续增强 产业互联网加速推进

详见《报告》

网络攻击和防护推动网络安全技术的发展

- Internet的应用覆盖了社会生活的方方面面，人类已经逐渐依赖计算机网络。
- 任何技术的发展给人们提高生活质量的同时，也不可避免地会被别有用心的人用于邪恶的目的。计算机和网络的发展为黑客的活动提供了舞台，导致了黑客攻击技术的发展。
- 为了应对黑客的攻击及其他安全威胁，安全研究人员致力于防护技术的研究，从而促进了网络安全防护技术的发展。
- **网络攻击和防护的对抗推动了网络安全技术的不断进步。**

1.4.2 网络安全技术的发展

- 早期的计算机主要是单机，应用范围很小，计算机安全主要是实体的安全防护和软件的正常运行，安全问题并不突出。
- 1970年代以来，人们逐渐认识到并重视计算机的安全问题，制定了计算机安全的法律、法规，研究了各种防护手段，如口令、身份卡、指纹识别等防止非法访问的措施。
- 为了对网络进行安全防护，出现了强制性访问控制机制、鉴别机制（哈希）和可靠的数据加密传输机制。
- 1970年代中期，Diffie和Hellman冲破人们长期以来一直沿用的单钥体制，提出一种崭新的双钥体制（又称**公钥体制**），这是现代密码学诞生的标志之一。

网络安全技术的发展

- 1977年美国国家标准局正式公布实施美国数据加密标准DES，公开DES加密算法，并广泛应用于商用数据加密，极大地推动了密码学的应用和发展。56位密码的DES 已经被破解，更高强度的密码技术取而代之，比如AES (Advanced Encryption Standard)，三重DES等。在我国应该推广AES的应用。
- 为了对计算机的安全性进行评价，80年代中期美国国防部计算机安全局公布了**可信计算机系统安全评估准则TCSEC**。准则主要是规定了操作系统的安全要求，为提高计算机的整体安全防护水平、研制和生产计算机产品提供了依据。

网络安全技术的发展

- Internet的出现促进了人类社会向信息社会的过渡。为保护Internet的安全，主要是保护与Internet相连的内部网络的安全，除了传统的各种防护措施外，还出现了防火墙、入侵检测、物理隔离等技术，有效地提高了内部网络的整体安全防护水平。

- 随着计算机网络技术的发展和应用的进一步扩大，计算机网络攻击与防护这对“矛”与“盾”的较量将不会停止。如何从整体上采取积极的防护措施，加紧确立和建设信息安全保障体系，是世界各国正在研究的热点问题。

网络安全技术的发展

- 为了从源头上解决计算机安全问题，近十几年来出现了可信计算机。“可信计算”成为了全世界计算机界的研究热点。它其实是信息安全问题的扩展，其基本问题与传统的信息安全问题仍然密切相关。
- 在2003前后，美国发起了**“软件验证大挑战”**运动，希望通过全球合作，验证100个重要基础程序的安全性与正确性，为此CAV每年举行一次国际学术会议。
- 目前，**云计算、移动计算和物联网应用**方兴未艾，然而其**安全问题令人担忧**。

1.4.3 黑客与网络安全

- 黑客技术与网络安全技术密不可分。计算机网络对抗技术是在信息安全专家与黑客的攻与防的对抗中逐步发展起来的。黑客主攻，安全专家主防。如果没有黑客的网络攻击活动，网络与信息安全技术就不可能如此快速的发展。
- **黑客一词是英文Hacker的音译**。一般认为，黑客起源于1950年代麻省理工学院的实验室中，他们是热衷于解决技术难题的程序员。在1950年代，计算机系统是非常昂贵的，只存在于各大高校与科研机构中，普通公众接触不到计算机，而且计算机的效率也不是很高。为了最大限度地利用这些昂贵的计算机，最初的程序员就**编写出了一些简洁高效的捷径程序**，这些程序往往较原有的程序系统更完善，而这种行为便被称为**Hack**。**Hacker指从事Hack行为的人**。

黑客

- 在1960和1970年代，“黑客”一词极富褒义。早期的**原始黑客代表的是能力超群的计算机迷**，他们奉公守法、从不恶意入侵他人的计算机，因而受到社会的认可和尊重。

- 早期黑客有一个精神领袖—凯文•米特尼克。早期黑客奉行**自由共享、创新与合作的黑客精神**。然而，现在的“黑客”已经失去了其原来的含义。虽然也存在不少原始意义上的黑客，但是当今人们听到“黑客”一词时，大多数人联想到的是那些以恶意方式侵入计算机系统的人。

黑客的三类行为特征

- “黑帽子黑客”(Black hat Hacker)、“白帽子黑客”(White hat Hacker)和“灰帽子黑客”(Gray hat Hacker)。

① **“黑帽子黑客”**是指只从事破坏活动的黑客，他们入侵他人系统，偷窃系统内的资料，非法控制他人计算机，传播蠕虫病毒等，给社会带来了巨大损失；

② **“白帽子黑客”**是指原始黑客，一般不入侵他人的计算机系统，即使入侵系统也只为了进行安全研究，在安全公司和高校存在不少这类黑客；

③ **“灰帽子黑客”**指那些时好时坏的黑客。

- **骇客是“Cracker”的英译**，是Hacker的一个分支，主要倾向于软件破解、加密解密技术方面。在很多时候Hacker与Cracker在技术上是紧密结合的，Cracker一词发展到今天，也有黑帽子黑客之意。

怎样才算一名黑客？

- 一个黑客首先需要在技术上得到大家的认可，在某项安全技术上拥有出众的能力，才能算是个黑客。此外，还需要具备自由、共享的黑客精神与正义的黑客行为。

- 总的来说，**要成为一个黑客必须是技术上的行家并且热衷于解决问题，能无偿地帮助其他人。**

黑客行为道德规范

- 真正的黑客拥有自己的职业道德，格守自己的行为规范，他们有着自己圈内的游戏准则，总结起来有如下几条：

(1) 不随便进行攻击行为

- 真正的黑客很少从事攻击行为，每当找到系统漏洞并入侵时，会很小心地避免造成损失，并尽量善意地提醒管时或帮系终打好安全补丁。他们不会随便攻击个人用户和站点。

(2) 公开自己的作品

- 一般黑客们所编写的软件等作品都是免费的，并且公开源代码，黑客们的作品不带任何商业性质，真正地做到了开源共享。

黑客行为道德规范（续）

(3) 帮助其他黑客

- 网络安全包含的内容广泛，没有哪个人能做到每一方面都精通，真正的黑客会很热心地在技术上帮助其他黑客。

(4) 义务地做一些力所能及的事情

- 黑客都以探索漏洞与编写程序为乐，但在圈内，除此之外还有很多其他的杂事，如维护和管理相关的黑客论坛、讨论组和邮件列表，维持大的软件供应站点等，这些事情都需要人做，但并非有趣。所一以，那些花费大量精力，义务地为网友们整理FAQ、写教程的黑客以及各大黑客站点的站长，他们都付出了大量的时间和精力，是值得尊敬的。

黑客精神

(1)**自由共享的精神**

- 这是**黑客文化的精髓**，是黑客精神最值得称赞的地方。自由共享是黑客应具备的最基本品质。

(2)**探索与创新的精神**

- 他们努力打破传统的计算机技术，努力探索新的知识，在他们身上有着很强的“反传统”精神。

(3)**合作的精神**

- 个人的力量是有限的，何况不可能精通任何网络安全方面的技术。黑客很明白这一点，因此他们乐于与他人交流技术，在技术上保守的人是不可能成为黑客的。

黑客必备的基本技能

- 作为一名黑客，需要有高超的技术；
- 计算机技术的发展日新月异，每天都有大量新的知识不断涌现，黑客们需要不断地学习、尝试新的技术，才能走在时代的前面。

作为一个黑客，必须掌握一些基本的技能：

(1)精通程序设计

- **一般来说，汇编、C语言都是黑客们应该掌握的。**

(2)熟练掌握各种操作系统

(3)熟悉互联网与网络编程

如何学习黑客技术

(1)兴趣是最好的老师

(2)学习黑客技术是一个长期的过程

(3)需要拥有一定的自学能力，主要靠自己。

黑客的发展历史

- **第一代黑客**
  - 第一代黑客在上个世纪50年代末至70年代初用“分时系统”技术把大型主机改造成了实际的个人计算机，使得更多的人有机会接触到计算机；
- **第二代黑客**
  - 第二代黑客在70年代发明并生产了个人计算机，领头人是苹果公司的创建人**史蒂夫·乔步斯**；
- **第三代黑客**
  - 第三代黑客为个人计算机设计出了各种应用、教育和娱乐程序，其中许多人后来成为80、90年代的软件设计师；

黑客的发展历史

- **第四代黑客**
  - 第四代黑客出现在80年代中期，他们促进并发展了Internet，并谋划使其变得更加开放和自由。黑客的行为已经形成了自己的文化，并接受社会实践的检验。黑客，从“妖魔”到“不速之客”，从个体到群体，其发展和演变十分神速。进入新世纪以来，有组织的黑客大战骤然升级，对抗次数频繁，其攻击手段和技术不断更新，阵容日渐壮大，其愈来愈向群体联盟化和社会化的方向发展并逐步成为举世关注的“焦点”。
- **现代黑客**
  - **重返自然状态，致力于对网络安全技术的研究。**
  - **很多黑客被政府招安，退出了黑客阵营。**

中国黑客发展史

- 从某种意义上来说，**中国没有黑客，或者说只有为数极少的黑客**，但网络上充斥着的**各种各样的工具造就了一批又一批的中国“伪黑客”。**

- **中国黑客在技术上与国外相比在很多方面存在明显的差距**，当然，这与国内的计算机和网络普及时间较晚有着一定的关系。

- 从1994年中国网民开始接触网络以来，中国黑客发展到现在一共经历了4代，也正是因为这些黑客的存在，才促使中国网民的安全意识逐渐提高，促使国内的网络安全行业逐渐发展。

1）中国黑客的起源(1994年—1996年)

- 也是中国互联网和计算机产业的起始时期。那时的计算机还是一件非常奢侈的电子用品，而互联网对于大众来说更是一个陌生的名词，只有在专业性极强的书刊中才能够找到与网络相关的名词，而那些上网的群体也多数为科研人员和年轻资本家（那个时候小资群体还没有提出）。
- 盗版还是一个陌生的名词，COPY就是正版的一种传播方式，软件的交换破解成为最为热门的话题—那个时代**最早的黑客或者说“窃客”诞生了，以破解软件和注册码为主**。
- 最早的交流是BBS，然后是互联网信息港。

窃客↔中国第一代黑客的雏形

- 1995年—1996年期间，中国各个大中城市的互联网信息港基本已经初具规模，中国国际互联网的第一代网管诞生，中国第一代的大众网民也开始走出BBS，融入天地更为广阔的Internet。

- 在这一期间中国网络窃客技术飞速发展，**以破解软件和注册码为主**。在那个阶段，除了窃客以外，电话飞客也曾出现在中国，但是由于程控交换机的出现，飞客很快成为了历史。1996年底，中国电信开始实行优惠上网政策，在此之后中国网络开始真正步入百姓家庭。

2）中国黑客的成长(1997年↔1999年)

- 此时“黑客”这一个名词已经开始正式的深入广大网友之中，当时初级黑客所掌握的最高技术仅仅是使用邮箱炸弹，并且多数是国外的工具，完全没有自己的黑客武器，更不要说自己的精神领袖。那个时期世界上的黑客追随着一个共同的精神领袖—**凯文•米特尼克**，世界头号黑客。这位传奇式人物不单单领导着美国黑客的思想，也影响着中国初级黑客的前进与探索方向。
- 1998年，出现“Back Orifice”的黑客软件，这个软件掀起了全球性的计算机网络安全问题，并推进了“特洛伊木马”这种黑客软件的飞速发展。

特洛伊木马和病毒的兴起

- BO并没有在中国掀起浪潮，主要原因是CIH病毒的诞生和大规模发作。这个有史以来第一个以感染主板BIOS为主要攻击目标的病毒给中国经济带来了数百亿元的损失。
- 由于排华、反华、台独以及美国轰炸中国驻南联盟大使馆事件，中国黑客被逐步打上了政治色彩，一直作为奋斗理想的美国黑客精神迅速的被遗弃了，中国红客开始出现。
- 众多优秀的国产黑客软件纷纷涌现，黑客也开始出现商业化迹象。
- 由前“绿色兵团”成员组建的“中联绿盟”网络安全公司成立，正式开始了黑客向商业化迈进的脚步，中国黑客逐渐成长了起来。

3）浮躁的欲望(2000年～2002年）走向2003

- 中国的黑客队伍也在迅速扩大着，众多的黑客工具与软件使得进入黑客的门槛大大降低，黑客不再是网络高手的代名词。也正是因为这种局面的出现，中国黑客的队伍开始杂乱。
- **伪黑客开始大量涌现**。对技术一窍不通的伪黑客以各种方式上演了一幕幕的闹剧，亵渎了中国黑客的精神。
- 这时国内的黑客基本分成三种类型：
  ① 一种是以中国红客为代表，略带政治性色彩与爱国主义情结的黑客；
  ② 一种是以蓝客为代表，他们热衷于纯粹的互联网安全技术，对于其他问题不关心的技术黑客；
  ③ 还有一种就是完全追求黑客原始本质精神，不关心政治，对技术也不疯狂追捧的**原色黑客**。

4）2003年以后：在惨败中反思
中国黑客重返自然状态

- 2001年4月，“中美撞机事件”导致**中美黑客网络大战，中国红客惨败!!!**

- **中国黑客在惨败中反思**，思想逐渐成熟，众多黑客纷纷**再次回归技术**，没有再热衷于媒体的炒作。

- 黑客道德与黑客文化的讨论和延伸也让中国黑客重返自然状态，致力于对网络安全技术的研究。

作业和实践

中国科学技术大学研究生信息平台

第1章作业