第1章
网络安全综述

中国科学技术大学

曾凡平

billzeng@ustc.edu.cn

第1章 网络安全综述

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、不可抵赖性**、**可用性和可控性**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（消息）的层面

网络和系统的层面

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，通过**信息隐藏**可以保证不暴露保密通信的事实。

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，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。
- 一般说来，系统的完整性如果得不到保护，数据的完整性也得不到保护。

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。

信息安全属性

(4)不可抵赖性(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。即：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。
- 技术：**审计和日志，数字签名和安全协议**

(5)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是否真实。**确保实体就是所声称的实体**。
- 技术：**标识和认证**

信息安全属性

(6) 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：**授权与访问控制等技术**。如：信息系统和网络边界的访问控制。

(7) 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。

- 技术：**安全审计与计算机取证等技术**

(8) 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系统的可靠性，但是平均无故障时间并不能完全保证系统的可靠性。

(9) 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：
  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

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。

网络安全体系结构的相关术语

(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**，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**。
- 安全策略（一套安全规则）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。

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

图1.1 分层的网络安全体系结构

可以将网络安全体系结构看作是**网络协议层次、安全功能和安全技术**的集合

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**安全属性**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安全属性。

1.2 计算机网络的脆弱性及面临的安全威胁

- 由于网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性，使得网络存在很多严重的脆弱性。

层和协议的集合称为网络体系结构（network architecture）

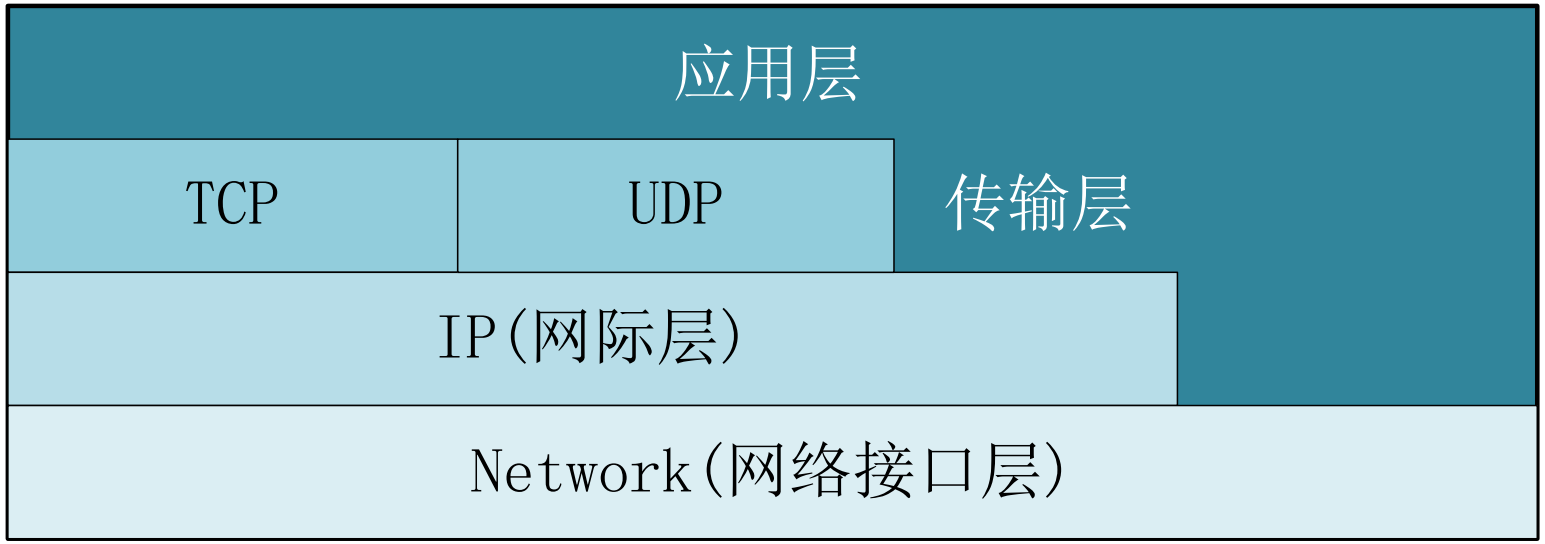


图1.2 TCP/IP网络体系结构

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3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。

nmap端口探测

nmap 192.168.86.200

PORT STATE SERVICE
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
21/tcp open ftp
25/tcp open smtp
42/tcp open nameserver
53/tcp open domain
80/tcp open http

nmap 192.168.86.122

PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11

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，以获得目标系统中安全漏洞的详细信息。**

- 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

nmap服务探测，通过服务判断漏洞

sudo nmap -sV 192.168.86.200

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd 5.0

80/tcp open http **Microsoft IIS httpd 5.0**

119/tcp open nntp Microsoft NNTP Service 5.00.0984

135/tcp open msrpc **Microsoft Windows RPC**

515/tcp open printer Microsoft lpd

548/tcp open afp (name: WIN2K-201501; protocol 2.2; MS2.0)

563/tcp open snews?

3389/tcp open ms-wbt-server Microsoft Terminal Services

Service Info: Host: win2k-201501; OSs: Windows, **Windows 2000**, Windows XP.....

用专业的软件进行漏洞探测

实例：物联网安全测评系统

- 物联网安全测评**系统的主要功能**：

1. **网关及云平台安全扫描**：扫描任务创建、执行、生成报告等
2. **移动应用安全评估**：APP的基础信息、危险API、权限等分析及恶意检测等
3. **嵌入式Web页面及API测试**：基于组合测试的错误定位、面向XSS的自适应随机测试
4. **固件安全分析**：静态分析固件，找出固件所包含的CVE漏洞


首页 - IoT安全测评
不安全 | 202.38.78.56:8333/home
百度翻译
邮件
Journal | IEEE Comp...
Learning
Research
Money
Teaching
Life
Developing
其他收藏夹
IoT安全测评
首页
网关测评
移动应用分析
嵌入式Web分析
物联网设备分析
测评结
任务列表
报告列表
报告分析
安全测评全流程、IoT组件全覆盖
对新一代智能物联网网关进行全面的安全测评，保证网关的服务安全。
开始使用
»SECURITY«


/gateway/
不安全
/gateway/scan/all_report_analysis
物联网安全测评平台数据分析
2022-09-02 17:48:57 星期五
任务状态数量
任务总数
5个
New 0个
Requested 0个
Running 0个
Done 5个
收录漏洞数量
发现的CVE漏洞数量
收录的CVE漏洞数量/每年
400
300
200
100
0
1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019
收录的漏洞危害性统计
总量
120352个
Log 23个
Low 9473个
Medium 88888个
High 21968个
发现的漏洞危害性统计
Log 253个
Low 2个
报告编号 所属扫描 测评时间 状态
7e034170-7807-4b26-8a74-a836c68b6f4b baidu 2022-08-22 12:42:59 Done
307e558f-4f53-4b70-a978-82578f24b2b3 alibaba 2022-08-22 12:53:30 Done
818c5416-f2b1-4111-be24-cad7eb8d0a0a alibaba 2022-08-25 20:40:03 Done
48027d79-c0ee-4f2d-9e9b-ea8ecaff337a localhost 2022-08-24 10:11:42 Done
收录的NVT脚本数量
0.0 3591个
0.1-3.9 1858个

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。

- **网络攻击的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

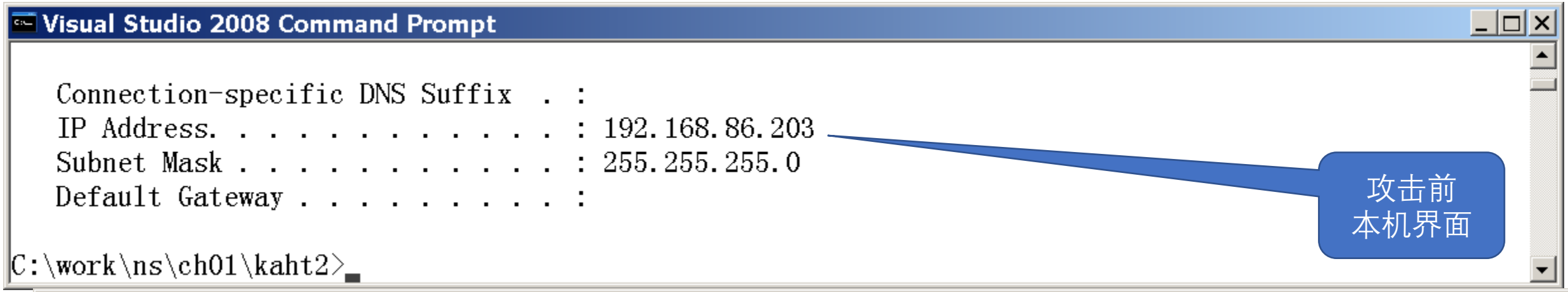
- **拒绝服务（Denial of Service, DoS）**攻击的主要目的是降低或剥夺目标系统的可用性，使合法用户得不到服务或不能及时得到服务，一般通过耗尽网络带宽或耗尽目标主机资源的方式进行。

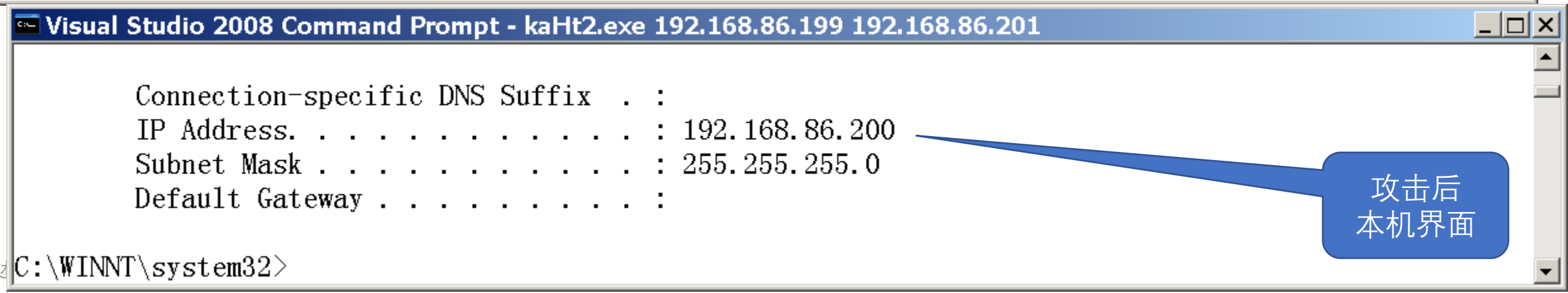
(2) 入侵攻击

- 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。
- 入侵攻击最常用的技术是攻击目标系统中存在**缓冲区溢出漏洞**的进程，在目标进程中执行**具有特定功能的代码**（称为**shellcode**），从而获得目标系统的控制权。

攻击实例：Windows 2000 RPC漏洞的远程缓冲区溢出攻击

- 从Windows 系统远程攻击具有RPC （缓冲区溢出）漏洞的系统
- 被攻击系统的IP：192.168.86.200
- 发起攻击的系统：Windows 2003 Server





网络攻击技术

(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。

网络攻击技术

(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

- 网络安全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。
- 网络安全防护的**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**，允许授权用户访问，阻止非授权用户进入网络，从而保证网络系统的**机密性、可控性**和**可用性等安全属性**；

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**；

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，使得破坏者走不掉，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**。

包过滤防火墙实例：linux系统内置防火墙

$ sudo ufw status

[sudo] password for i:
Status: active

To	Action	From
22/tcp	ALLOW	Anywhere
10022	ALLOW	Anywhere
10060:10079/tcp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
10022 (v6)	ALLOW	Anywhere (v6)
10060:10079/tcp (v6)	ALLOW	Anywhere (v6)

ufw 是Ubuntu 系统自带的防火墙管理命令

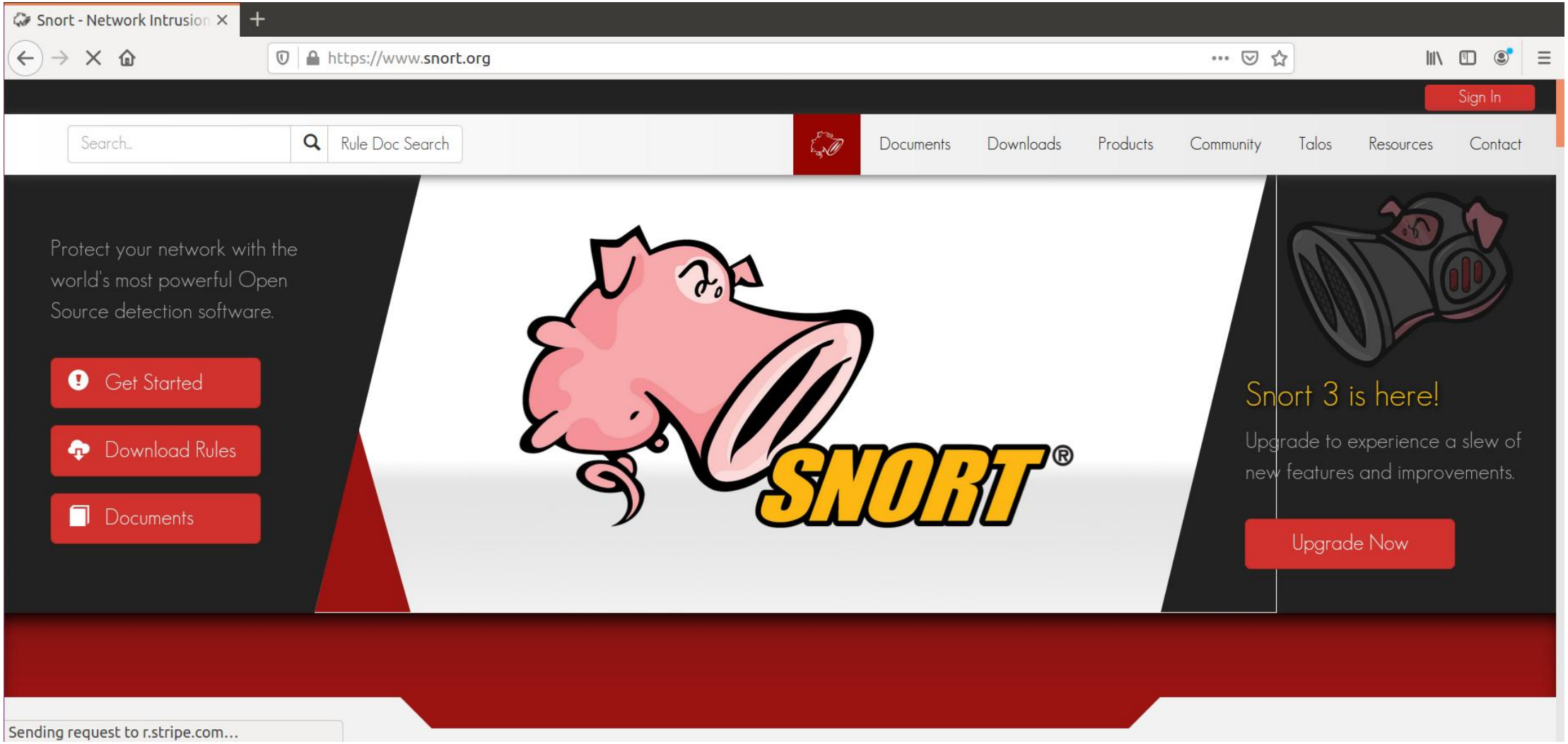
(2)入侵检测技术

- 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响应。
  - ✓如果在IDS的基础上加上防火墙的实时阻断功能，就成为**入侵防护**技术**IPS**（实际上是**入侵检测+防火墙**）。IDS一般是离线运行的，而IPS要实现实时阻断，因此要求具备快速实时的能力，在超高速网络上不容易实现。

- 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。

入侵检测系统实例：
snort： https://www.snort.org/



(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) 密码技术和虚拟专用网技术

- 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的重要机制，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**。
- 虚拟专用网VPN技术基于密码技术，在公共网络上构建安全隧道以保证数据的机密性和完整性，包括**远程访问VPN**和**网关—网关VPN**。

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程中是否被窜改、重放或延迟等。
- 数字签名是实现信息认证的主要技术。

(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。
- “蜜罐”上的监控器和事件日志器可检测未经授权的访问并收集攻击者活动的相关信息。

1.4 网络安全的起源与发展

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56次《中国互联网络发展状况统计报告》发布

- 2025年7月21日，中国互联网络信息中心（CNNIC）在京发布第56次《中国互联网络发展状况统计报告》（以下简称《报告》）。
- 《报告》显示，“十四五”期间，我国互联网建设取得显著成就。新型信息基础设施加速布局，互联网基础资源持续丰富，为互联网普及和数字经济发展提供了坚实支撑。
- 截至6月，我国网民规模达11.23亿人，互联网普及率达79.7%，越来越多的群体共享数字发展成果。
- 新兴市场蓬勃发展，人工智能技术应用加速落地，全球影响力不断提升，科技创新引领经济社会高质量发展。

- 详见：https://cnnic.cn/n4/2025/0721/c88-11328.html

网络攻击和防护推动网络安全技术的发展

- 互联网络的应用规模巨大，这些应用覆盖了社会生活的方方面面，人类已经逐渐依赖互联网络。
- 任何技术的发展在提高人们生活质量的同时，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，1980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。**

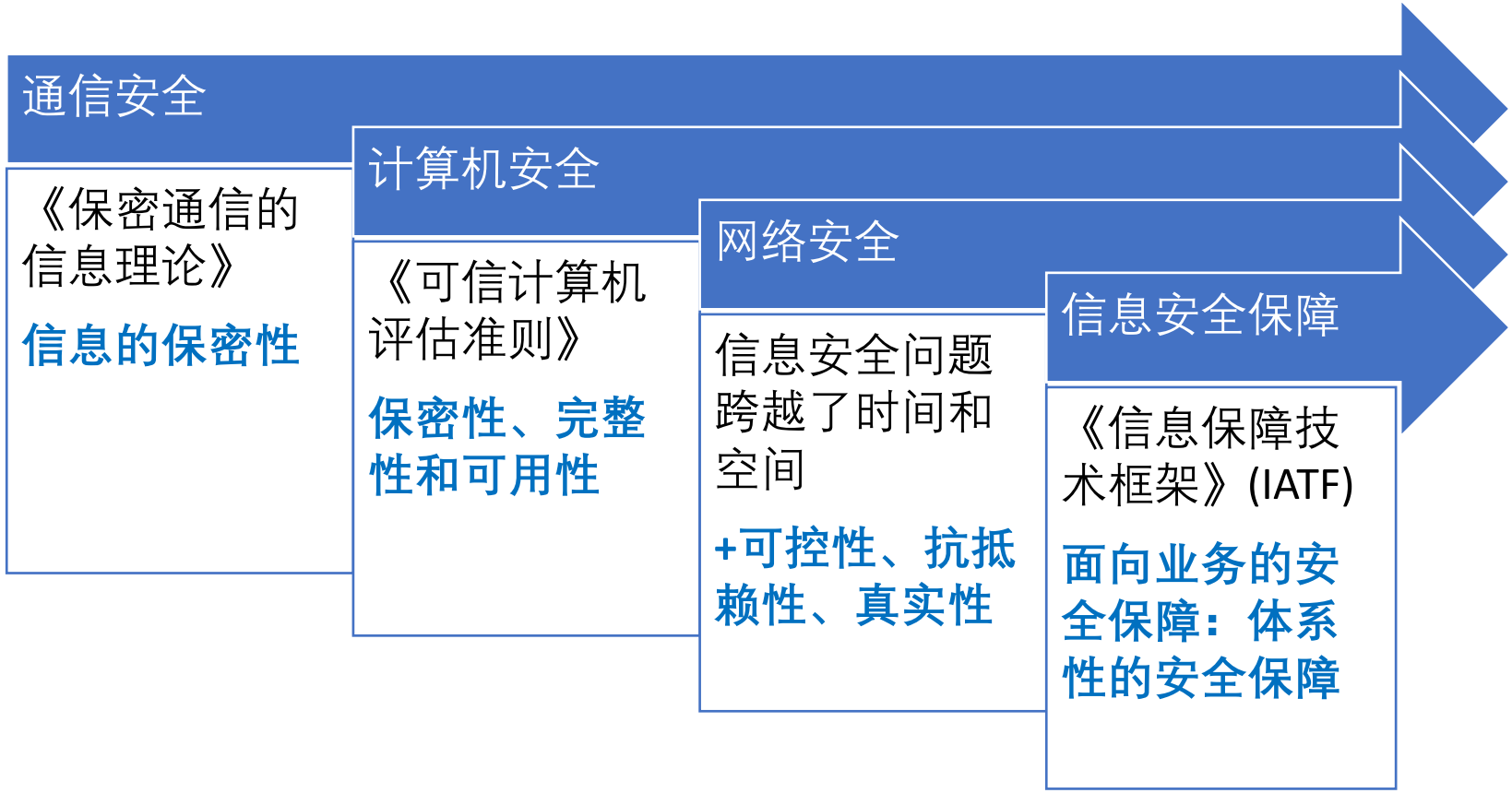
网络安全技术的发展

- 为了从源头上解决计算机安全问题，近二十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，**人工智能**技术飞速发展，然而其**安全问题令人担忧**。

网络与信息安全的4个发展历程

大体上，网络与信息安全发展经历了4个时期



网络信息安全的发展是层层递进的，不是替代式的发展、而是累积式的发展

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《**可信计算机系统评估准则**》（Trusted Computer System Evaluation Criteria，**TCSEC**，俗称橘皮书，1985年再版）为标志。
- 在20世纪60年代后，数据的传输已经可以通过网络来完成，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，信息无论是在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

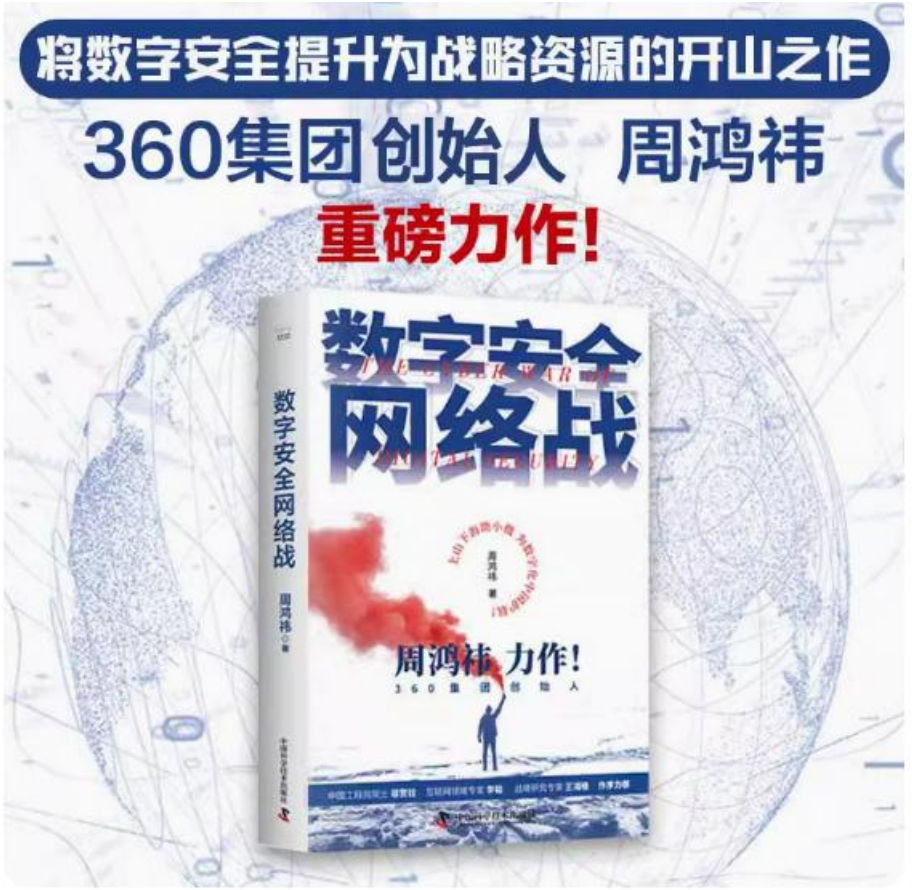
- 21世纪的信息安全保障时代，其主要标志是**《信息保障技术框架》(IATF)**。
- **面向业务的安全保障：体系性的安全保障理念**，不仅是关注系统的安全漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。
- 面向业务的安全保障不是只建立防护屏障，而是建立一个**“深度防御体系”**，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动地防御攻击。
- 也就是说，面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为**从整体角度考虑其体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

新观点：数字文明时代的数字安全

- 国家提出数字中国战略，世界加速向数字文明时代迈进。
- 数字化是继工业革命之后的，最重要的生产力革命。

- 数字文明时代的信息安全，从网络安全拓展到数字安全(或是一般意义上讲的网络安全)。

- 参考：360集团创始人周鸿祎的**《数字安全网络战》**。



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**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**。

关于黑客（about Hacker）

- 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。

中国“红客”

- “红客”是中国特殊历史时期的产物，是指那些具有强烈爱国主义精神的黑客，以宣扬爱国主义红客精神为主要目标。“红客”成立于1999年5月，标志事件是第一个中国红客网站—“中国红客之祖国团结阵线”的诞生，导火线是美军轰炸中国驻南联盟大使馆。
- “红客”主导了1999年和2001年的两次“中美黑客网络大战”，可惜当时的中国黑客整体技术水平不如美国黑客，**中国黑客在2次“中美黑客大战”中惨败**。
- 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。

1.4.4 计算机网络战-军方的观点

- 计算机网络战是在网络空间内进行的对抗，有时也称为**赛博空间战（Cyberspace Warfare）**：

- 这种对抗形式是通过计算机通信网络，**截取、利用、篡改、破坏**对方的信息，利用假冒信息或病毒等来危害对方的信息与信息设施，并同时保护己方的信息与信息基础设施，以达到预期目的的行动。

- **美国是最早从事网络战研究的国家：**
  - **美国陆军从1994年就开始实施数字化部队建设。**
- 先有计算机对抗，后有计算机网络战。
- 计算机网络战是信息战的一个重要组成部分，它是夺取和保持战场制信息权的一种主要作战手段。
- 美军的网络战准备：
  - 1995年1月至6月，美国著名的兰德公司和国防部设计了6次网络战演习；1995年6月，美军16名“第一代网络战士”从美国国防大学新设立的信息战学院毕业。此后，网络战成为美军的首要战备之一。
- 1991年海湾战争的网络战。
- 科索沃战争（1999年3月24日~6月10日）中的网络战。
- 俄乌战争中的网络战。
  - 请参考周鸿祎编著的**《数字安全网络战》第1章**

美军从“平台中心战”向“网络中心战”演变

- 二十一世纪的战争是信息战争，而“网络战”又必将成为信息战争的更重要组成部分。在未来战争中谁掌握了“制网络权”，谁便掌握了“制胜权”，便可以实现“不战而屈人之兵，决胜于千里之外”的最高战争境界。

- 新世纪必然要从“平台中心战”向“网络中心战”(美国人提出的)演变

- 2009年6月前后，美国向全世界宣告，成立**网络战司令部**，标志美国从“平台中心战”向“网络中心战”的战略转型。

我国的《国家网络空间安全战略》

- 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》

- 《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攻击技术的研究提升为国家战略。
- 详见：**《国家网络空间安全战略》**（全文20161227）
- 本课程介绍网络攻击和防护技术，主要目的是提高学员的网络安全意识，提高安全防护能力。

谢谢！