网络安全概述改

第一章　网络安全

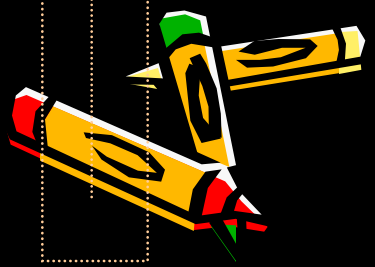
- 1.0　引言
- 1.1　网络安全的基本知识
- 1.2　网络面临的安全威胁
- 1.3　网络安全防护体系
- 1.4　网络安全的发展

本章学习目标

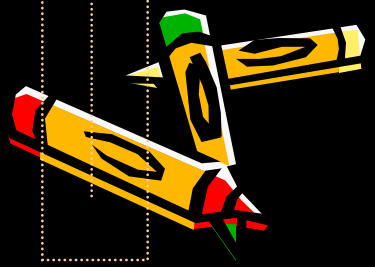
- （1）网络安全的含义、目标
- （2）网络安全的研究内容
- （3）网络存在的安全威胁及存在安全威胁的原因
- （4）网络安全防护体系
- （5）网络安全的发展、现状及趋势

1.0 引言

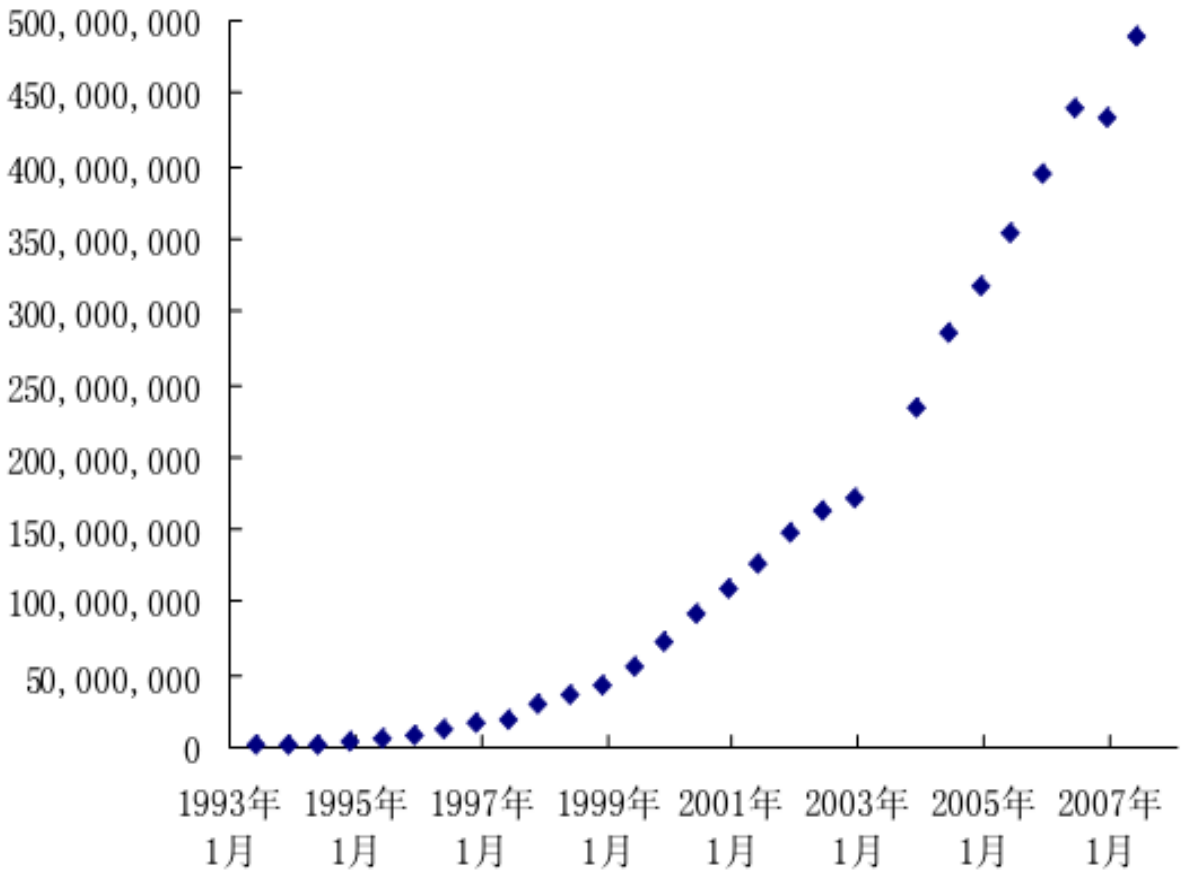
看一些统计数据和具体事件



第1章 网络安全



Internet软件联盟统计的全球互联网主机的数量



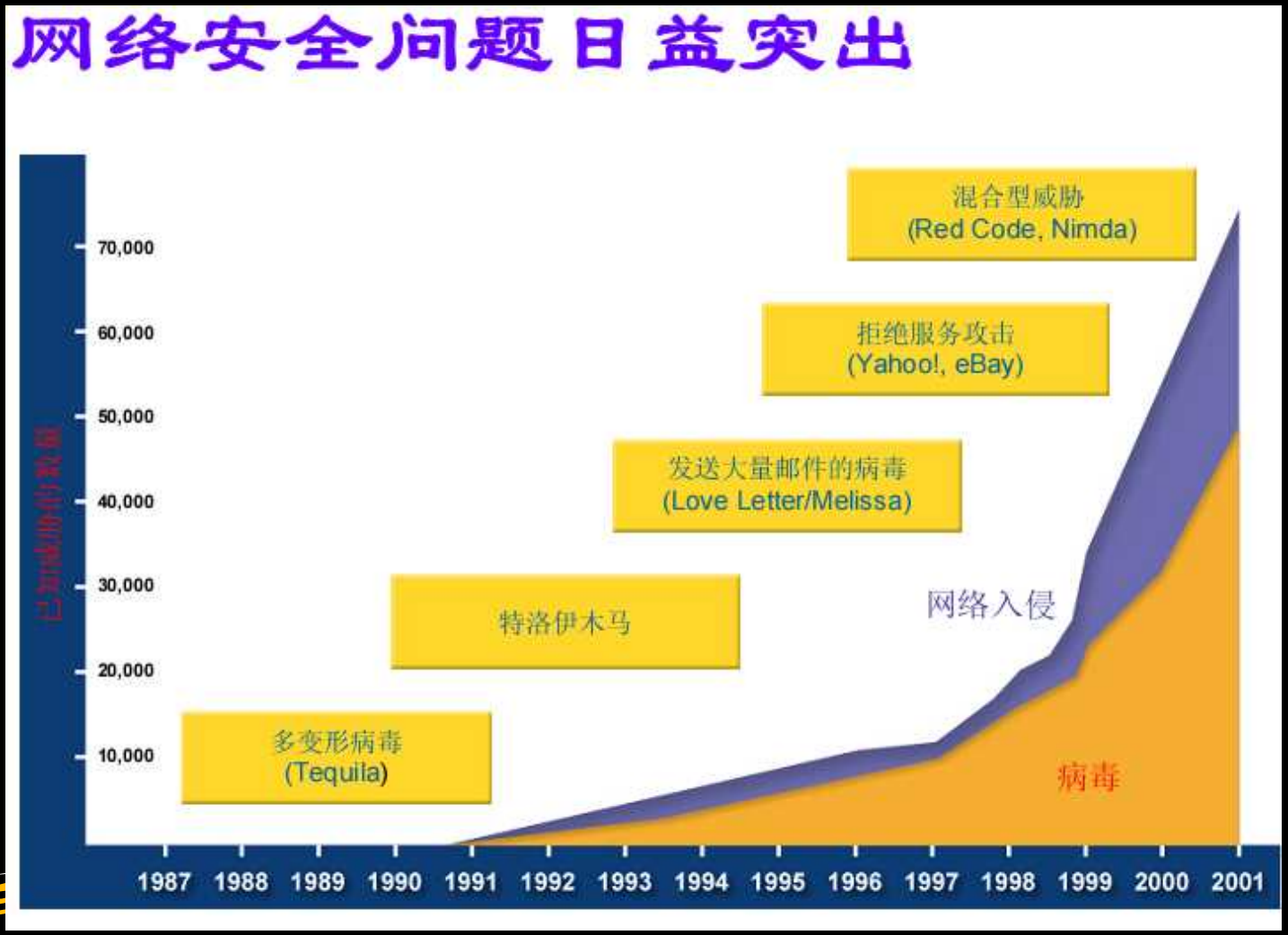
中国网民规模和年增长率



中国网民上网计算机数


中国网民规模和年增长率
万人
网民人数
网民规模年增长率
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
80%
70%
60%
50%
40%
30%
20%
10%
0%
4580
5910
6800
7950
8700
9400
10300
11100
12300
13700
16200
72.8%
75.4%
48.5%
34.5%
27.9%
18.2%
18.4%
18.1%
19.4%
23.4%
31.7%
2002.06
2002.12
2003.06
2003.12
2004.06
2004.12
2005.06
2005.12
2006.06
2006.12
2007.06

网络安全问题日益突出


混合型威胁
(Red Code, Nimda)
拒绝服务攻击
(Yahoo!, eBay)
发送大量邮件的病毒
(Love Letter/Melissa)
特洛伊木马
多变形病毒
(Tequila)
网络入侵
病毒
70,000
60,000
50,000
40,000
30,000
20,000
10,000
1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001

CERT有关安全事件的统计



- 1993年，中国科学院高能物理研究院建设了一个试验性质的网络，开通不久，一名欧洲黑客发现了这个陌生的地址并闯进来，成为中国第一个黑客案例。
- 2019年，中国最老牌的黑客组织"绿色兵团"成立，黑客从此有了自己的江湖。
- 2019年5月，印度尼西亚发生排华事件，一群愤怒的黑客向印尼网站发起攻击。
- 2019年5月8日美国"误炸"中国驻南使馆后，美国的一些政府网站,包括能源部,内政部在内,这些网站的首页上一度高高飘扬着五星红旗.白宫的网站失灵3天.

以色列最机密核项目遭到“木马”病毒入侵

- 东方网2005年6月11日消息：以色列近日刚破获一起利用“特洛伊木马”病毒的工业间谍案。据称它的一个秘密核目在严密看护下竟遭到“特洛伊木马”病毒的侵入。

黑客入侵 台湾否认外交部泄密

- 2005年7月1日，台湾媒体报道指出，外交部网站遭黑客侵，疑是大陆“网军”所为，窃取台湾外交机密文件；
- 《联合报》并引述未具名的行政院官员透露指出，大陆面透过木马程序一再入侵台湾公务部门，包括国防部网等，也曾入侵民进党中央，了解民进党高层的出访动向。

2019中美黑客大战（被黑美网站图片）




fuck USA Government
fuck PoizonBOx


Microsoft Internet Explorer
http://www.zackspro.com
中华人民永不向侵略者低头
Chinese people will never bow to the aggressor
打倒美国霸权主义
Bowl down the hegemonicism of United State
布什政府＝流氓的政府
Bush-administration = blackguardly government
中华人民共和国公民:冷怒——LZJYW
Citizen of People's Republic Of China——lzjyw
load home page : fuck U.S.A
Internet


Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
地址(D)
转到

美军设立网络战司令部

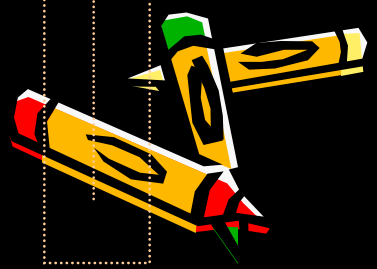
- 美国国防部长罗伯特·盖茨2009年6月23日正式下令设立美国军方网络司令部，以协调国防部防御网络攻击、展开网络战的行动

各国网络战部队现状

- 美国
  目前拥有最大的网络战力量，三军都有网络部队。
- 英国
  英国军情六处早在2019年就秘密组建了一支由数百名计算机精英组成的黑客部队。
- 日本
  日本防卫省已经组建了一支由计算机专家组成的约5000人的网络战部队，专门从事网络系统的攻防。该部队的主要任务是，进行反黑客、反病毒入侵的攻击，同时研制开发可破坏其他国家网络系统的跨国性"网络武器"，必要时可对敌方重要网络实施"瘫痪战"。

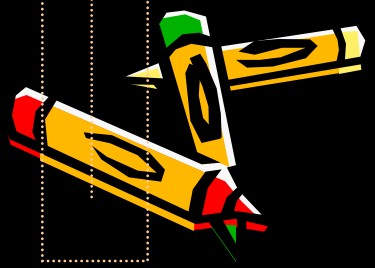
好了，
这个环节就介绍到这了

continue



1.1 网络安全的基本知识

- 1.1.1 网络安全的基本概念
- 1.1.2 网络安全目标
- 1.1.3 网络安全缺陷
- 1.1.4 网络安全的研究内容
- 1.1.5 常见网络攻击方法



1.1.1 网络安全的基本概念

- 是指保护网络系统的硬件、软件及其数据不受偶然的或者恶意的原因所导致的破坏、更改、泄露， 使系统连续可靠正常地运行，网络服务不中断。
- 从广义上来说，凡是涉及到网络上信息的机密性、完整性、可用性、真实性、抗否认性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全从其本质上来讲就是网络上的信息安全(包括通信保密、信息安全、信息保障)。

2、网络安全

一般可以认为网络安全包括物理安全、运行安全和数据安全三个层次，它们涵盖的范围如图1-1所示。

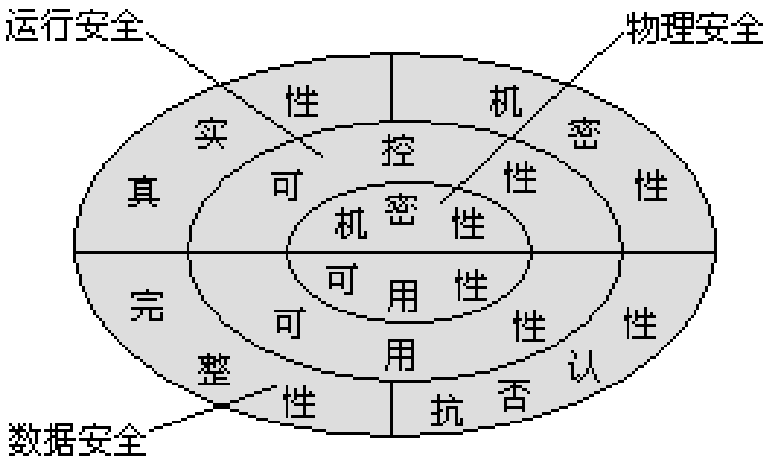


图 1-1　网络安全涵盖的范围

网络安全的含义是指通过各种计算机、网络、密码技术和信息安全技术、网络控制技术，保护网络中传输、交换、处理和存储的信息的机密性、完整性、可用性、真实性、抗否认性和可控性。

3、网络安全观

（1）网络安全是网络动态发展的问题。

（2）网络安全实施是一个系统工程。

（3）网络安全实施是一个社会工程。

所以说，网络安全是一个动态发展的系统工程和社会工程，需要长期、持久的巨大财力、物力、人力的投入，需要从组织、管理等方面采取强有力的措施，才能确保网络在信息的大洋中永远坚固、安全、可靠。

1.1.2 网络安全目标

在ISO7498-2开放系统安全架构中提出，要解决网络安全问题，主要是在四方面提供服务，而IATF则近一步演化为安全的六性。

1．机密性　　2．完整性

3．可用性　　4．抗否认性

5．可控性　　6．真实性

1.1.3 网络安全缺陷

1. 普遍存在的安全缺陷

（1）网络的规模。

（2）电磁辐射和电磁泄漏。

（3）搭线。

（4）串音。

2. 中国特色的安全缺陷

（1）由技术被动性引起的安全缺陷。

（2）人员素质问题引起的安全缺陷。

（3）缺乏系统的安全标准所引起的安全缺陷。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/127160201114006054