专业特色选修课《网络信息安全》

概念篇

网络信息安全概述

Introduction to Network and Information Security

嵩　天

songtian@bit.edu.cn

北京理工大学计算机学院

本节大纲

- 网络信息安全态势现状
- 网络信息安全概念和特性

斯诺登事件

- 事件
  - 2013年6月9日，爱德华•斯诺登
  - 《卫报》和《华盛顿邮报》
  - 美国、中国香港、俄罗斯、玻利维亚
- 《世界人权宣言》第十二条
  - “任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击。人人有权享受法律保护，以免受这种干涉或攻击。”

技术&责任

“反应了美国“自由”、“民主”、“人权”说教的虚伪性”

心脏滴血事件

- 事件
  - 2014年4月9日，OpenSSL的Heartbleed漏洞
  - SSL是最为普遍的网络加密技术，攻击全球2/3服务器
  - 攻击者可以利用漏洞连接客户端或服务器的存储器内容，从而读取用户信息等内容
  - 漏洞编号：CVE-2014-0160
- 分析

安全问题不可避免

  - 基于缓冲区溢出的漏洞是目前网络入侵的最主要手段
  - 概念设计安全和系统实现安全存在鸿沟

glibc事件

- 事件
  - 2015年1月28日，glibc发现严重安全漏洞，幽灵漏洞
  - glibc 提供系统调用和基本的C函数库，比如malloc, printf等
  - 攻击者通过gethostbyname系列函数实现远程代码执行，获取服务器的控制权及Shell权限，几乎覆盖所有的Linux版本
  - 漏洞编号：CVE-2015-0235
- 分析
  - 发现或不发现，漏洞就在那里

安全问题一直存在

本节大纲

- 网络信息安全态势现状
- 网络信息安全概念和特性

人类对安全的需求

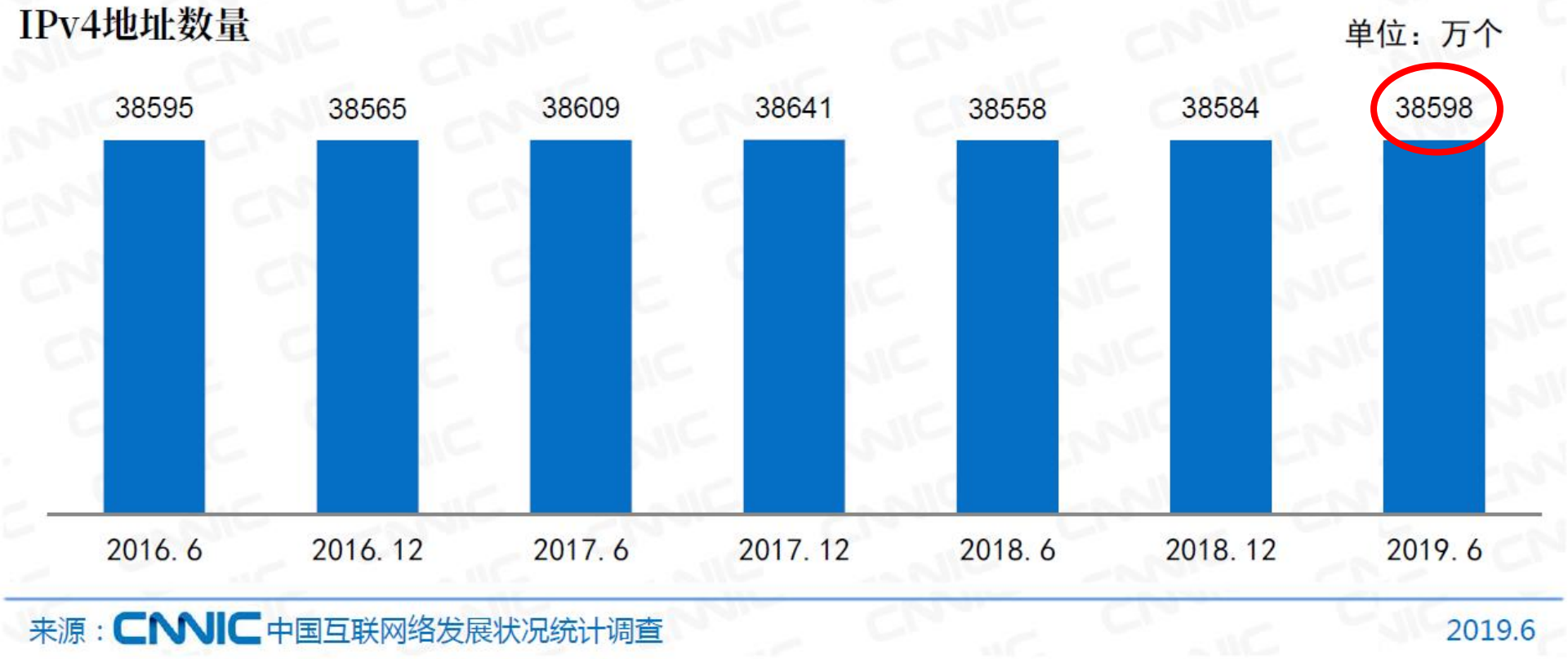
- 需求层次理论
  - 美国心理学家马斯洛（Maslow）首创的一种理论
  - 《人类动机的理论》，1943年
  - 人最迫切的需要才是激励人行动的主要原因和动力
- 网络信息安全是人类安全需求的重要组成部分

从数字认识安全现状

- 从解读一系列数字开始，来源如下：
  - 2019年8月，《中国互联网络发展状况统计报告》
  - 2020年1月，CNCERT互联网安全威胁报告
  - 国家信息安全漏洞共享平台(CNVD)安全周报
  - 国家计算机病毒应急处理中心病毒检测周报

数字和趋势是思考未来的关键!

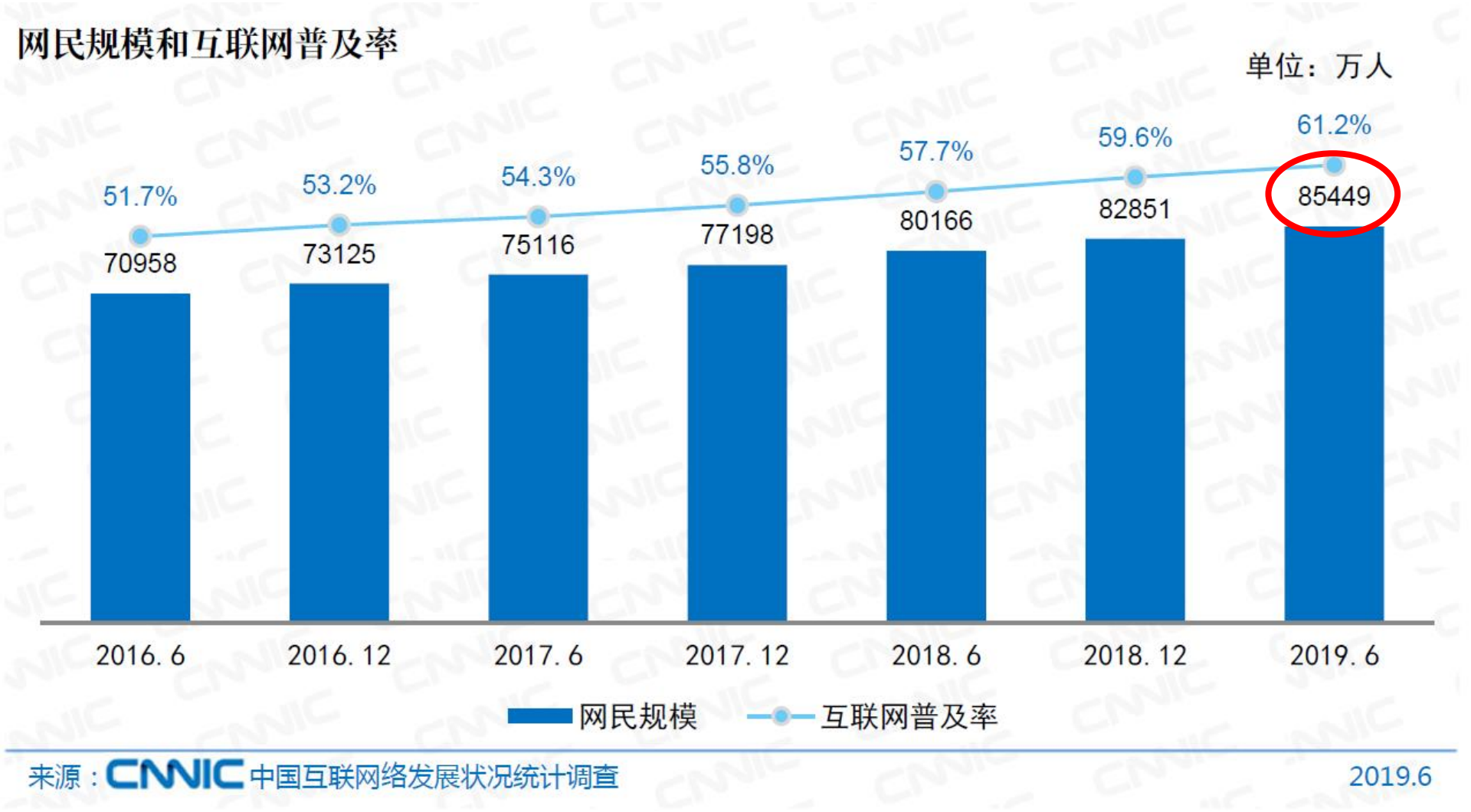
从数字认识安全现状


IPv4地址数量
单位：万个
38595
38565
38609
38641
38558
38584
38598
2016. 6
2016. 12
2017. 6
2017. 12
2018. 6
2018. 12
2019. 6
来源：CNNIC 中国互联网络发展状况统计调查
2019.6

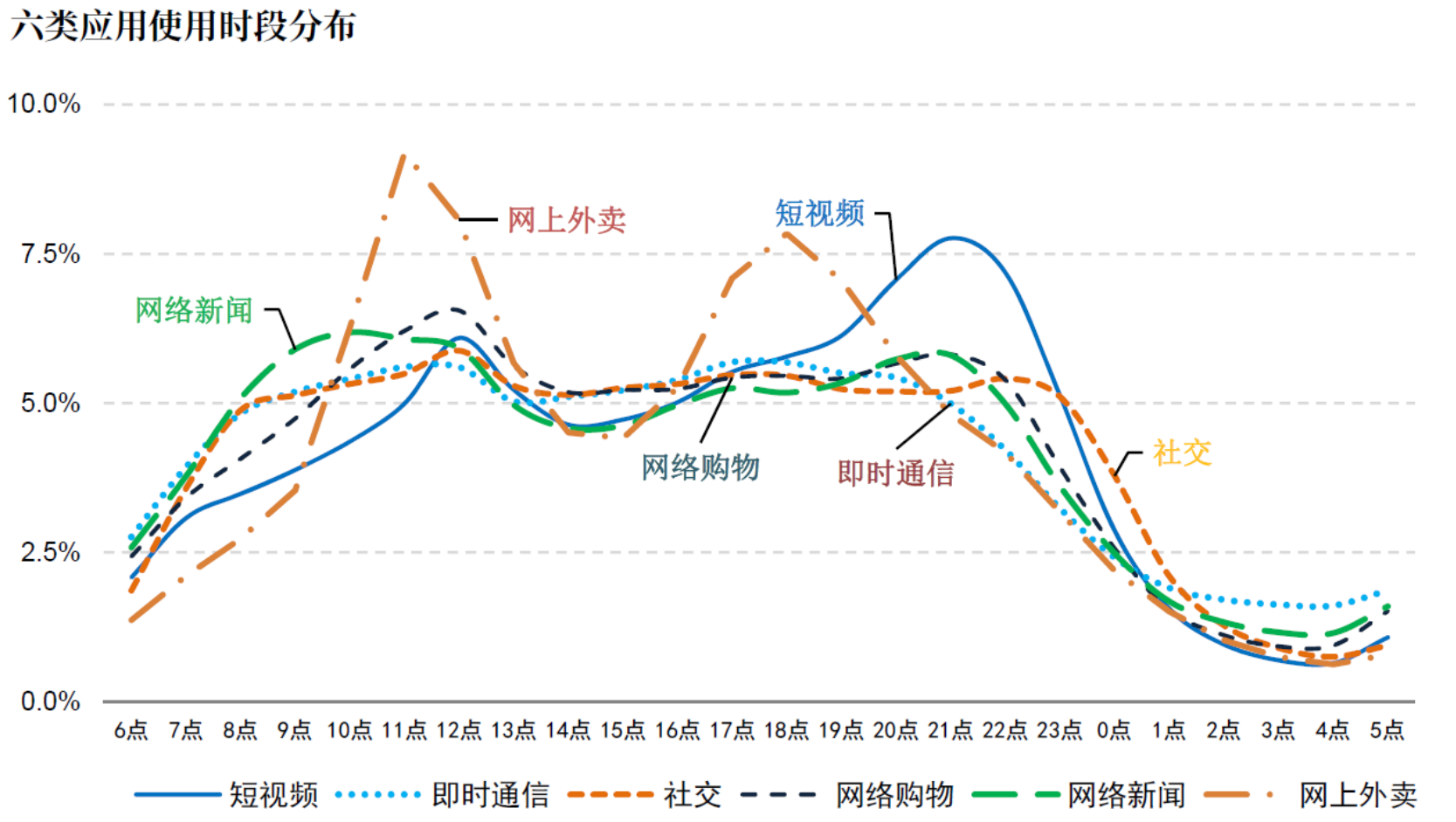
从数字认识安全现状

来源：CNNIC 中国互联网络发展状况统计调查 2019.6

从数字认识安全现状

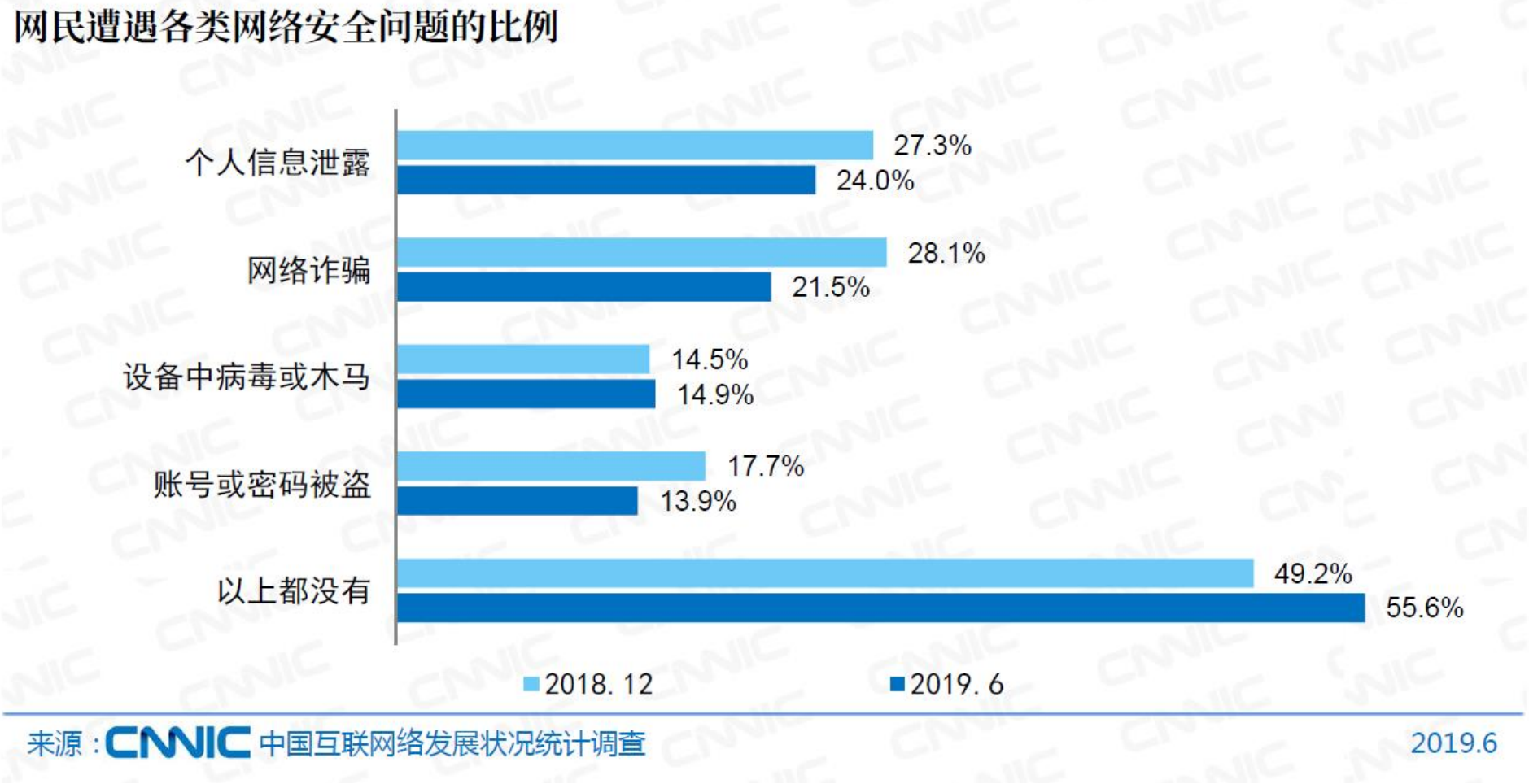

网民规模和互联网普及率
单位：万人
51.7%
53.2%
54.3%
55.8%
57.7%
59.6%
61.2%
70958
73125
75116
77198
80166
82851
85449
2016. 6
2016. 12
2017. 6
2017. 12
2018. 6
2018. 12
2019. 6
网民规模
互联网普及率
来源：CNNIC 中国互联网络发展状况统计调查
2019.6

从数字认识安全现状



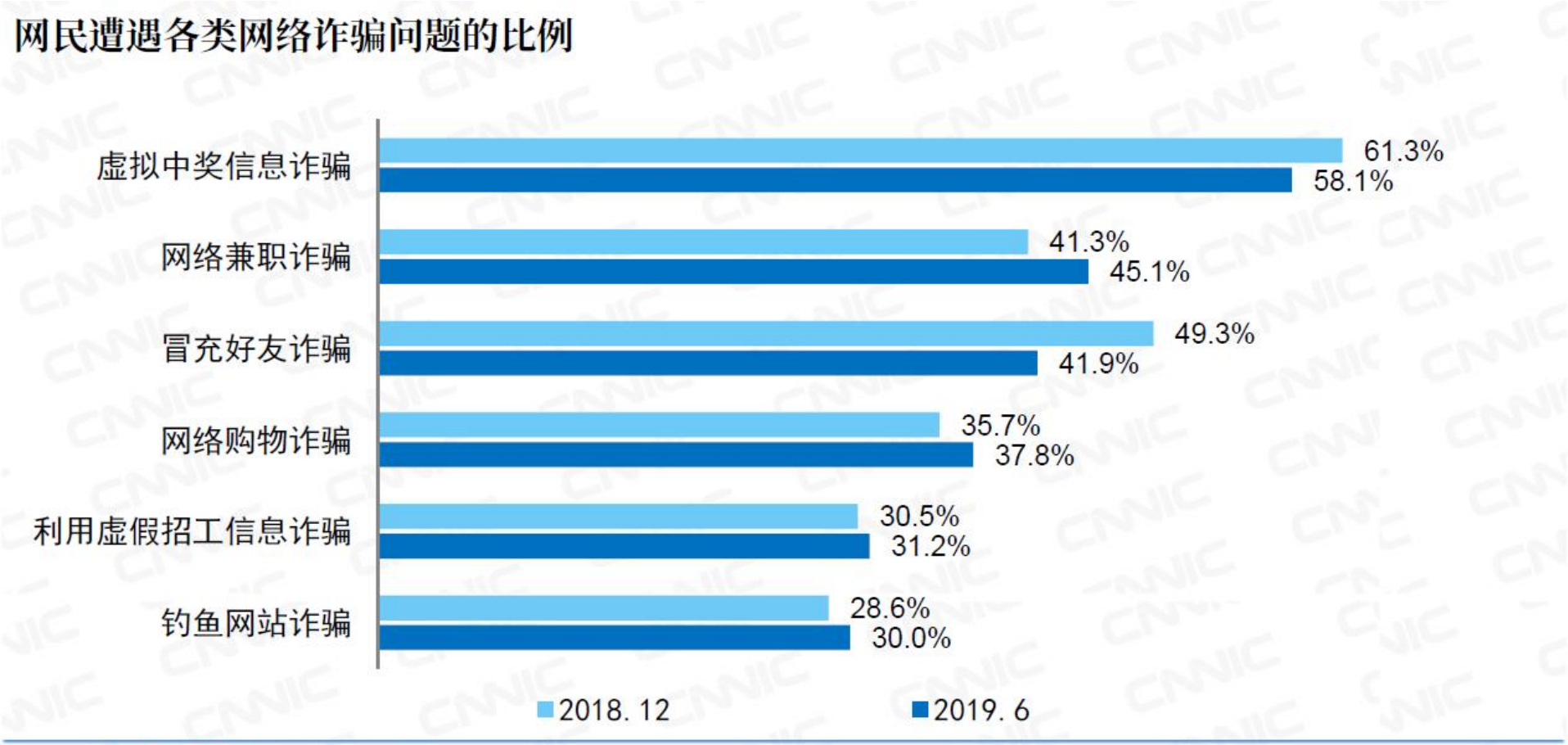
来源：中国电信 2019.6

从数字认识安全现状

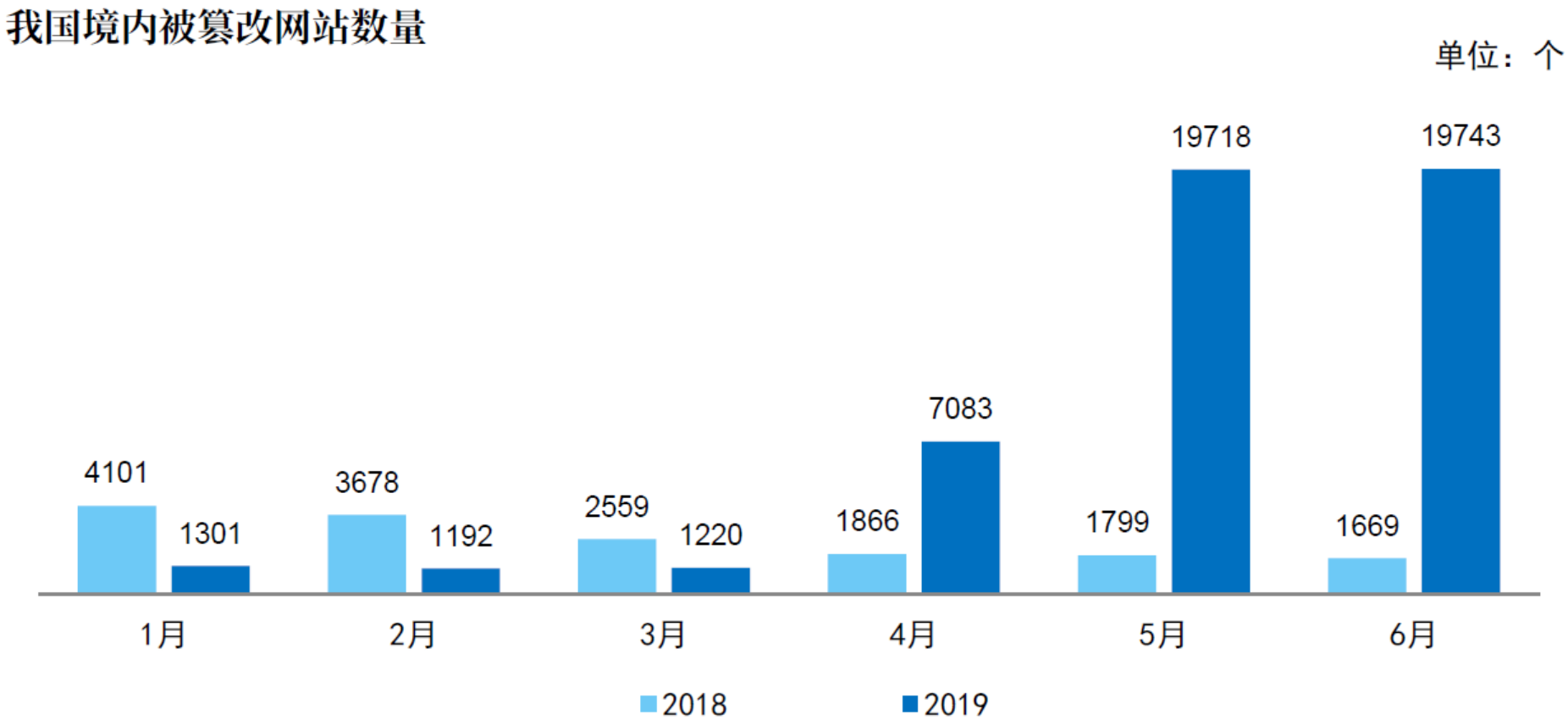


2019年，总网民中44.4%遭遇过网络安全问题

从数字认识安全现状


网民遭遇各类网络诈骗问题的比例
虚拟中奖信息诈骗
61.3%
58.1%
网络兼职诈骗
41.3%
45.1%
冒充好友诈骗
49.3%
41.9%
网络购物诈骗
35.7%
37.8%
利用虚假招工信息诈骗
30.5%
31.2%
钓鱼网站诈骗
28.6%
30.0%
2018. 12
2019. 6
来源：CNNIC 中国互联网络发展状况统计调查
2019.6

从数字认识安全现状



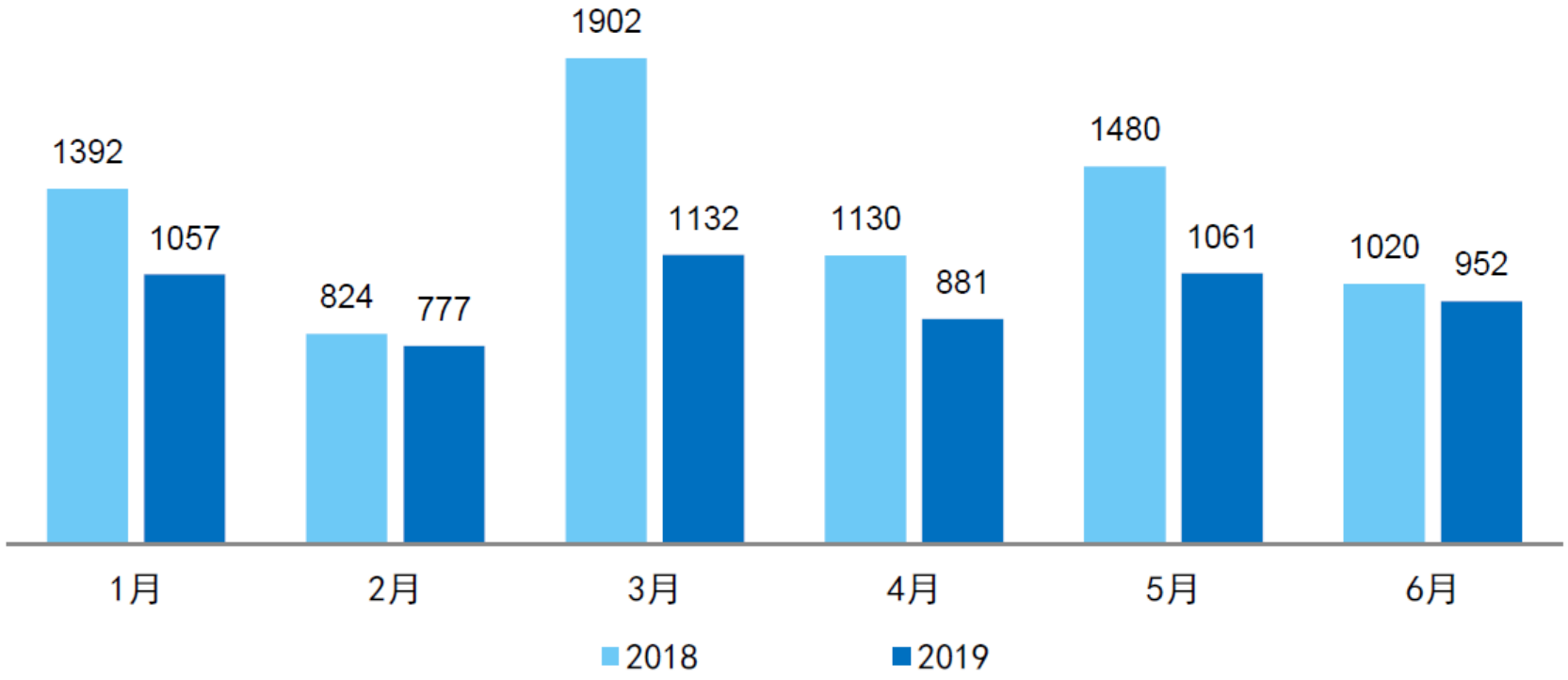
来源： CNCERT

2019.6

从数字认识安全现状

国家信息安全漏洞共享平台收录信息系统安全漏洞数量

单位：个



来源： CNCERT

2019.6

从数字认识安全现状

2020 年 1 月，互联网网络安全状况整体评价为良。主要数据如下：

- 境内感染网络病毒的终端数为近143万个；
- 境内被篡改网站数量为30,651个，其中被篡改政府网站数量为113个；境内被植入后门的网站数量为9,356个，其中政府网站有36个；针对境内网站的仿冒页面数量为815个；
- 国家信息安全漏洞共享平台(CNVD)收集整理信息系统安全漏洞1,047个。其中，高危漏洞409个，可被利用来实施远程攻击的漏洞有881个。

网络信息安全现状

- 网络信息安全发展的几个阶段
  - 通信保密阶段 （Communication Security）

    20世纪初期，侧重于密码学，研究通讯安全为主
  - 信息安全阶段 （Information Security）

    20世纪60年代，以保密性、完整性和可用性为目标
  - 网络信息系统安全阶段 （Information Assurance）

    20世纪90年代，从整体角度考虑体系建设的信息保障阶段
  - 现在是… (移动互联网安全阶段？安全失控阶段?)

网络信息安全现状

- 网络威胁有哪些？

网络信息安全现状

- 网络信息安全的一些经典结论
  - 公理1 所有的程序都有缺陷。（摩菲定理）
  - 定理1 大程序的缺陷甚至比包含的内容还多。
    - 推理1-1 一个安全相关程序有安全性缺陷。
  - 定理2 只要不运行这个程序，是否有缺陷，也无关紧要。
  - 定理3 对外暴露的计算机，应尽可能少地运行程序，且运行的程序也应尽可能小。

网络信息安全趋势

- 1. 集团化、产业化趋势 （国家化）
  - 产业链

    病毒木马编写者->专业盗号人员->销售渠道->玩家
  - 不再安于破坏系统，销毁数据，而更关注财产和隐私
  - 电子商务成为热点，针对网络银行的攻击更加明显

网络信息安全趋势

- 2. “黑客”逐渐变成犯罪职业
  - 财富的诱惑，使得黑客袭击不再是一种个人兴趣，而是越来越多的变成一种有组织的、利益驱使的职业犯罪

网络信息安全趋势

- 3. 恶意软件转型
  - 我国仍然是恶意软件最多的国家
  - 恶意软件在行为上将有所改观，病毒化特征削弱，手段更加“高明”，包含更多的钓鱼欺骗元素
  - 事件：
    - 网上大量出现的钓鱼网站

网络信息安全趋势

- 曾出现过的某假冒银行网站，网址为 http://www.1cbc.com.cn，而真正银行网站是 http://www.icbc.com.cn。
- 某假公司网站，网址为 http://www.1enovo.com，而真正网站为 http://www.lenovo.com。诈骗者通过QQ散布“XX集团和XX公司联合赠送QQ币”的虚假消息，引诱用户访问。

网络信息安全趋势

- 4. 网页挂马危害继续延续
  - 网络木马传播的“帮凶”
  - 服务器端系统资源和流量带宽资源大量损失
  - 客户端的用户个人隐私受到威胁

网络信息安全趋势

- 5. 一剑封喉：应用软件漏洞攻击
  - 新的漏洞出现要比设备制造商修补的速度更快
  - 一些嵌入式系统中的漏洞难以修补
  - 入侵和渗透的工具更加成熟

网络信息安全趋势

- 6. Web2.0的产品将受到挑战
  - 以博客、论坛为首的web2.0产品将成为病毒和网络钓鱼的首要攻击目标
  - 自动邮件发送工具日趋成熟，垃圾邮件制造者正在将目标转向音频和视频垃圾邮件
  - 社区网站上带有社会工程学性质的欺骗往往超过安全软件所保护的范畴

网络信息安全趋势

- 社会工程学
  - 一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段。
  - 社会工程学陷阱就是通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。

网络信息安全趋势

- 社会工程学

Your Email Address Has Won

Superenalotto [claimsunit@sbcglobal.net]

发送时间: 2009-9-26 (星期六) 19:23

收件人: undisclosed recipients:

Sir/Madam,

Superenalotto is the biggest lottery organization in Italy and with the prize in our jackpot going up and up we are now going international and picking winners worldwide. You have been selected via your email address as a winner in our internet draw to receive the prize of one million euro.

To claim and for further information contact us at claimdept01@alice.it
Your claim reference number is PAL/SPLM/09. Quote this when you contact us.

Thank you.
Claim Co-ordinator
Superenalotto Italy

网络信息安全趋势

- 7. 隐私泄露和网络舆论是安全发展的新趋势
  - 博客、微信、微博等泄露大量个人隐私，并被利用
  - 网络舆论容易被引导和误导，网络推手和投票公司的出现使得网络舆论引发信任危机
  - 网络舆情引发突发公共事件，对网络舆情的安全带来新的挑战（自然社会和网络社会相互影响）

网络信息安全趋势

- 两高司法解释

《最高人民法院 最高人民检察院 关于办理利用信息网络实施诽谤等刑事案件 适用法律若干问题的解释》

http://www.court.gov.cn/qwfb/sfjs/201309/t20130913_187998.htm

认定为“情节严重”：“同一诽谤信息实际被点击、浏览次数达到五千次以上,或者被转发次数达到五百次以上的”

网络信息安全趋势

- 集团化、产业化趋势
- “黑客”逐渐变成犯罪职业
- 恶意软件转型 -> 钓鱼网站
- 网页挂马危害继续延续
- 利用应用软件漏洞的攻击将更为迅猛
- Web2.0的产品将受到挑战
- 隐私泄露和网络舆论

网络信息安全趋势

- 8. 其他安全趋势
  - 高级可持续威胁攻击，APT (Advanced Persistent Threat)
  - 移动网络和移动用户
  - BYOD(Bring You Own Device)和企业安全
  - HTML5 和Web安全
  - 云计算、IPv6等安全问题
  - 工业控制计算机的安全问题

本节大纲

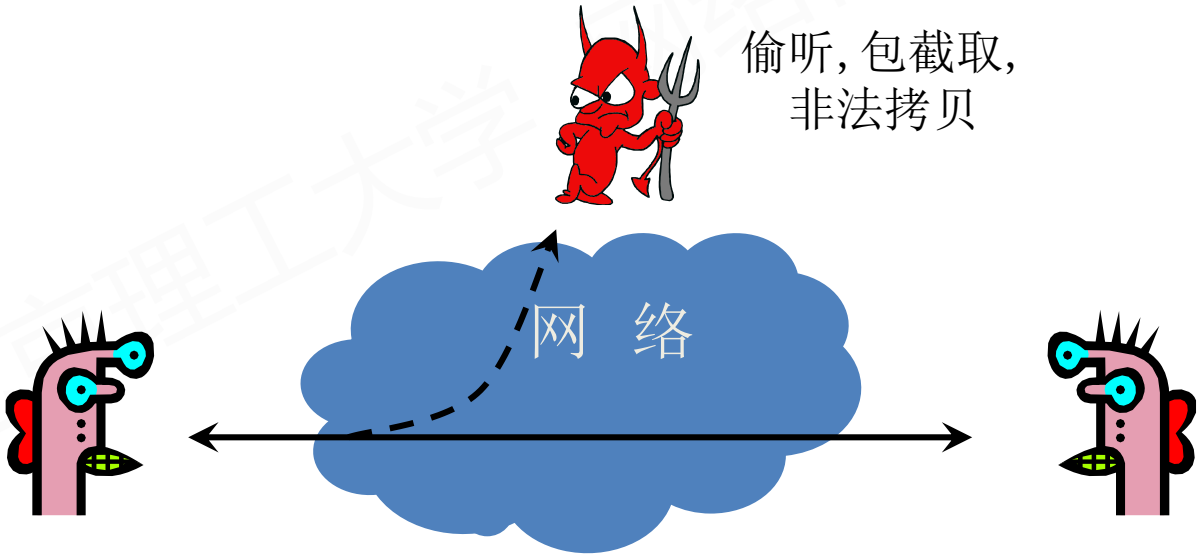
- 网络信息安全态势现状
- 网络信息安全概念和特性

网络信息安全概念和特点

- 网络安全的特点

机密性、完整性、可用性、可控性、不可否认性

– 机密性：杜绝有用信息泄露给非授权个人或实体；

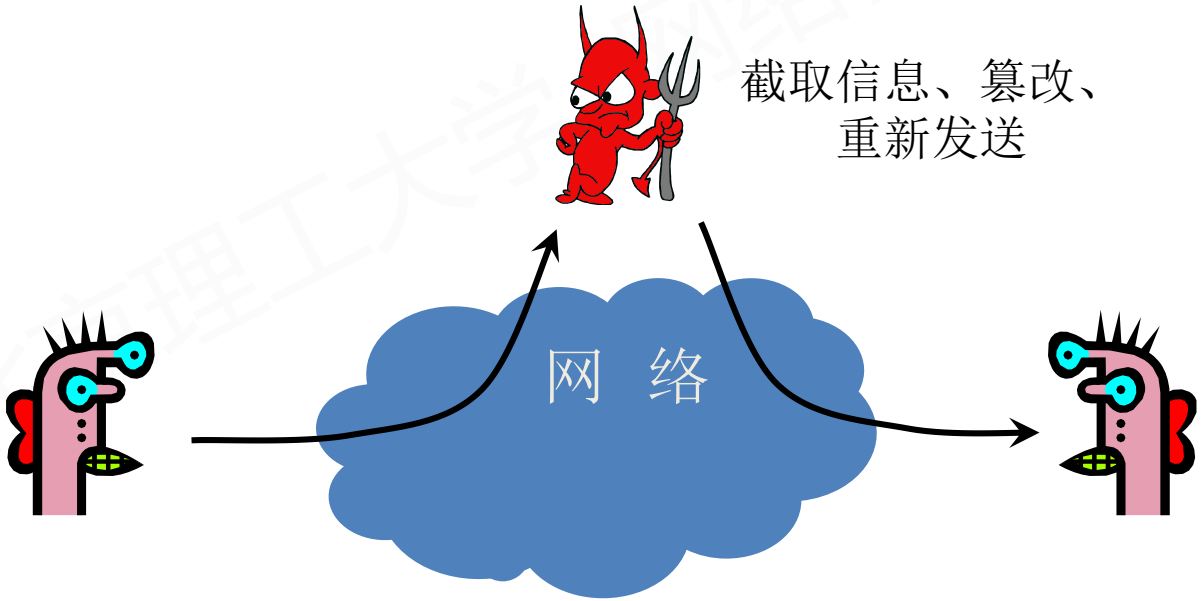


网络信息安全概念和特点

- 网络安全的特点

机密性、完整性、可用性、可控性、不可否认性

– 完整性：信息保持非修改、非破坏和非丢失；



网络信息安全概念和特点

- 网络安全的特点

机密性、完整性、可用性、可控性、不可否认性

– 可用性：可被授权实体正确访问；

网络信息安全概念和特点

- 网络安全的特点

机密性、完整性、可用性、可控性、不可否认性

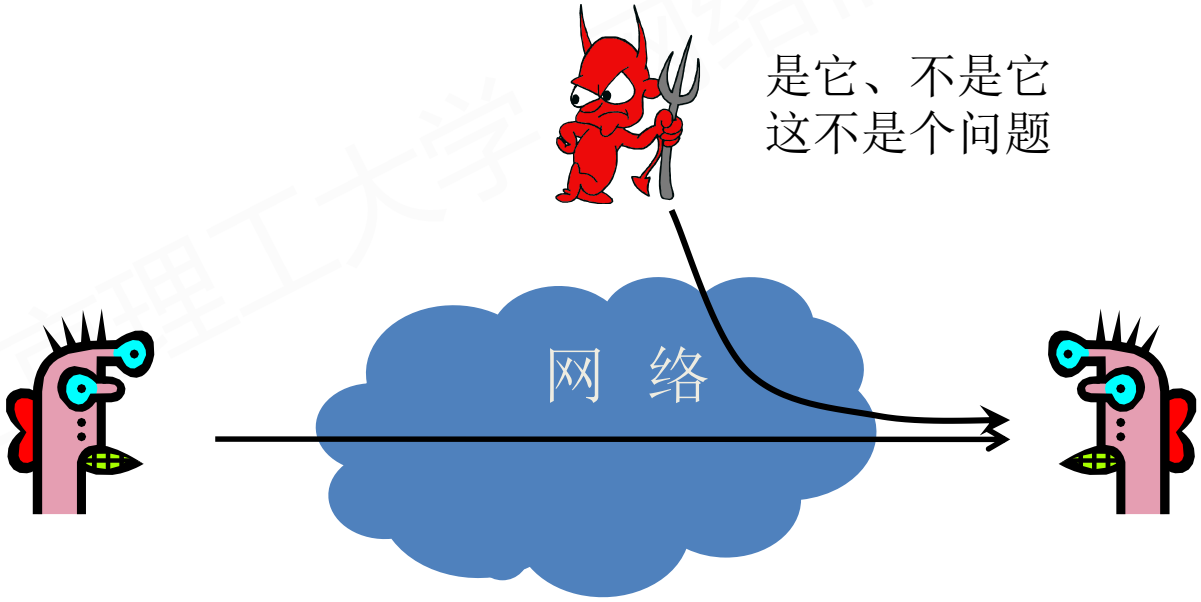
– 可控性：对网络中信息传播及内容能实现有效控制；

网络信息安全概念和特点

- 网络安全的特点

机密性、完整性、可用性、可控性、不可否认性

– 不可否认性：所有参与者不可否认或者抵赖本人的真实身份。



总结

- 网络信息安全在信息时代的重要性
- 我国网络信息安全现状
- 网络与系统的脆弱性和安全威胁类型
- 理解网络安全的五个特点