

第1章 计算机 网络安全概述

计算机网络安全技术

1.1 网络安全简介

1.2 网络安全所涉及的内容



学习目标

1.1.1 网络安全为什么重要

网络应用已渗透到现代社会生活的各个方面；电子商务、电子政务、电子银行等无不关注网络安全。网络安全上到国家安全，下至每个人的生活。信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防，称为cyber-space。



1.1.2 信息安全的概念

从本质上讲，网络安全就是网络上的信息安全，是指网络系统的硬件、软件和系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

广义上讲，凡是涉及到网络上信息的保密性、完整性、可用性、真实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。



1.1.2 信息安全的概念



网络安全的五要素



保密性—
confidentiality



完整性—
integrity



可用性—
availability



可控性—
controllability



不可否认性—
Non-repudiation

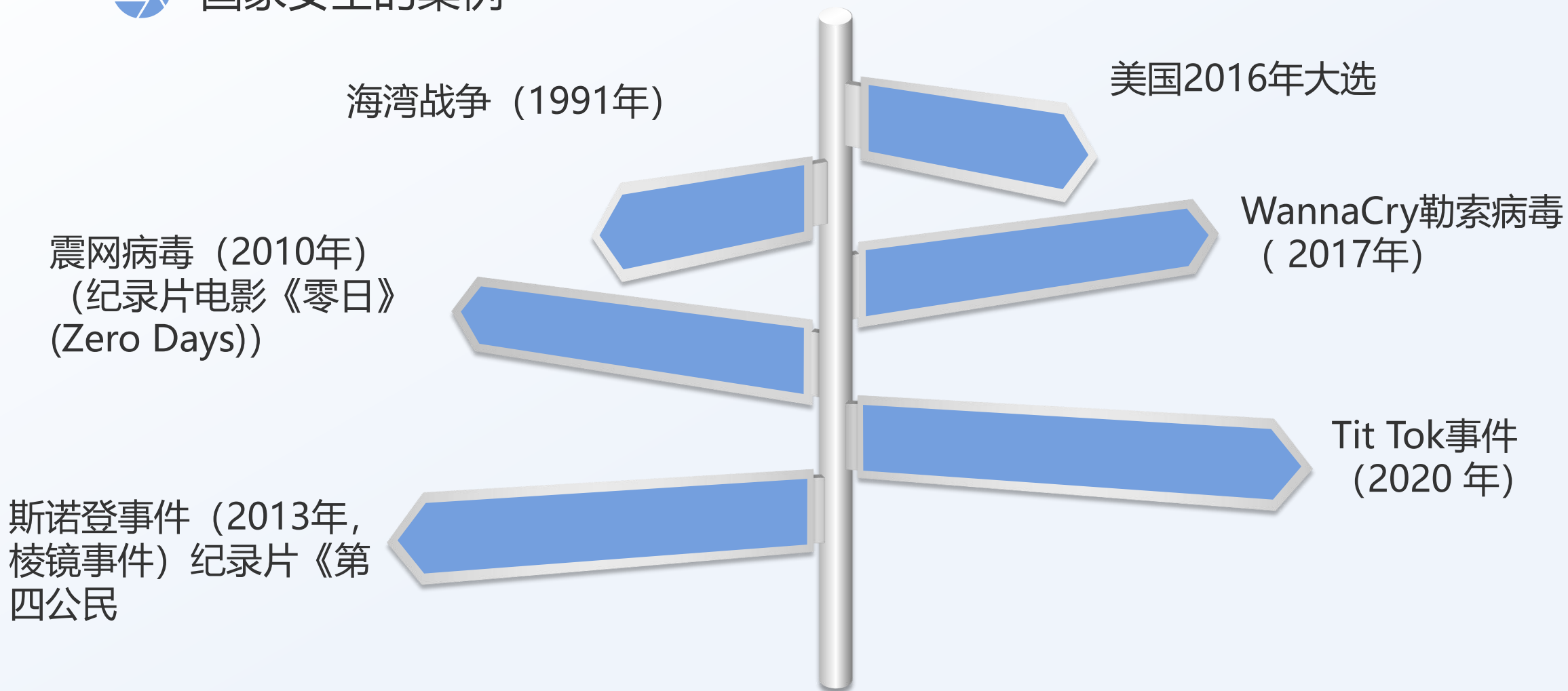
保密性（confidentiality）与Integrity（完整性）和 Availability（可用性）并称为信息安全的CIA三要素。



1.1.2 信息安全的概念



国家安全的案例



1.1.2

信息安全的概念

全国移动APP安全性研究报告：约70%的APP都存在安全漏洞

爱加密123

2019-05-07 17:39:29

192575

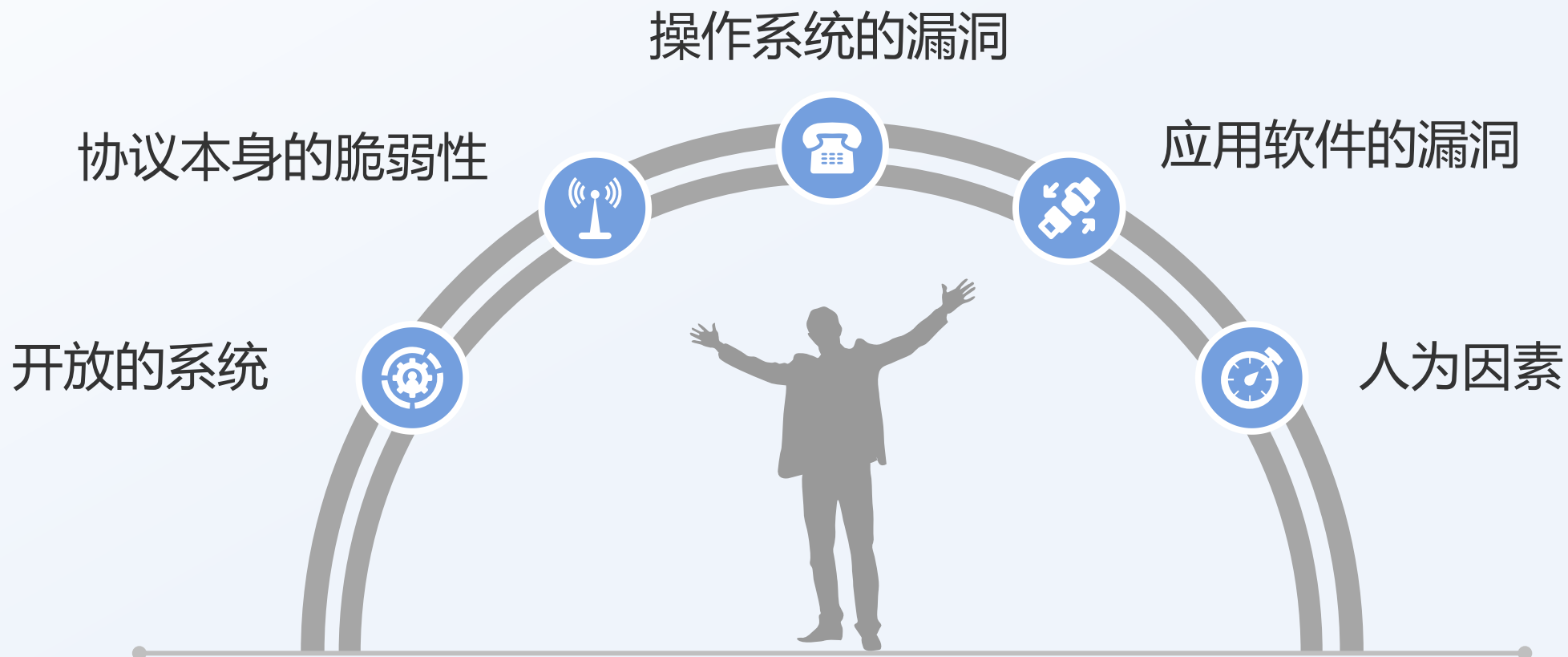
6

***本文中涉及到的相关漏洞已报送厂商并得到修复，本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担。**

据统计，每年至少新增150万种移动恶意软件，至少造成超过1600 万件的移动恶意软件攻击事件。爱加密全国移动 APP 安全性研究报告，旨在让移动手机用户了解 APP 风险隐患对个人隐私信息及资金安全等方面所造成的威胁，提高其安全防范意识。通过对 App 违法违规收集使用个人信息行为的通报，协同有关主管部门、APP 供应商、APP 提供商等，共同营造安全的移动应用环境，促进网络安全的规范化、安全化、健康化发展。

1.1.2 信息安全的概念

网络安全脆弱性原因



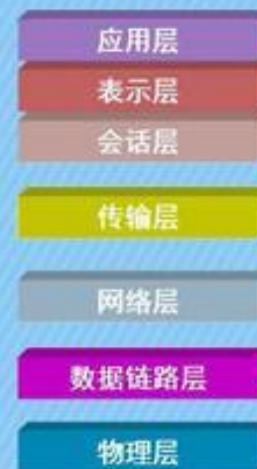
1.1.2 信息安全的概念

开放



在因特网上没有人知道你是一条狗。

开放系统互连参考模型



1.1.2 信息安全的概念

TCP/IP协议结构

| OSI | | TCP/IP协议集 | |
|-------|------|--|--|
| 应用层 | 应用层 | Telnet, FTP, SMTP, DNS, HTTP 以及其他应用协议 | |
| 表示层 | | | |
| 会话层 | | | |
| 传输层 | 传输层 | TCP , UDP | |
| 网络层 | 网络层 | IP, ARP, RARP, ICMP | |
| 数据链路层 | 网络接口 | 各种通信网络接口（以太网等） （物理网络） | |
| 物理层 | | | |



1.1.2

信息安全的概念

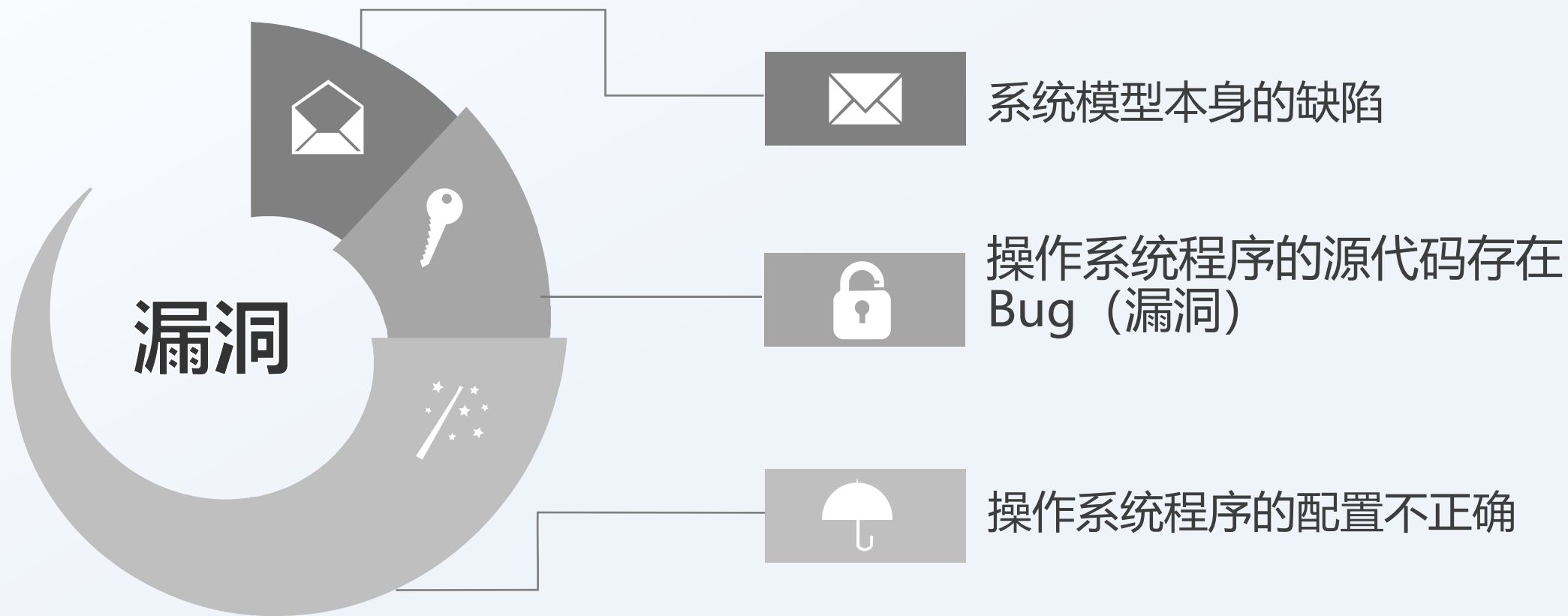
| 层 | 协议名称 | 攻击类型 | 原因 |
|-----|----------|--------------|--------------|
| 网络层 | ARP | ARP欺骗 | ARP缓存的更新机制 |
| | IP | IP欺骗 | IP层数据包是不需要认证 |
| | ICMP | ICMP Flood攻击 | 利用Ping |
| 传输层 | TCP | SYN Flood攻击 | TCP三次握手机制 |
| | UDP | UDP Flood攻击 | UDP非面向连接的机制 |
| 应用层 | FTP、SMTP | 监听 | 明文传输 |
| | DNS | DNS Flood攻击 | DNS的递归查询 |
| | HTTP | 慢速连接攻击 | HTTP的会话保持 |



1.1.2

信息安全的概念

操作系统存在的漏洞



1.1.2 信息安全的概念



微软漏洞分级

微软将安全漏洞按严重程度分为：紧急、重要、警告、注意四种。

最严重的是“紧急”级别。这一漏洞“如果被恶意使用，几乎不用做什么操作就可以造成大规模危害”

Windows 更新



更新可用

上次检查时间: 昨天, 8:37

2020-08 适用于 Windows 10 Version 1909 x64 的 .NET Framework 3.5 和 4.8 的累积更新预览 (KB4570723)

状态: 正在等待下载

已有更新可供下载

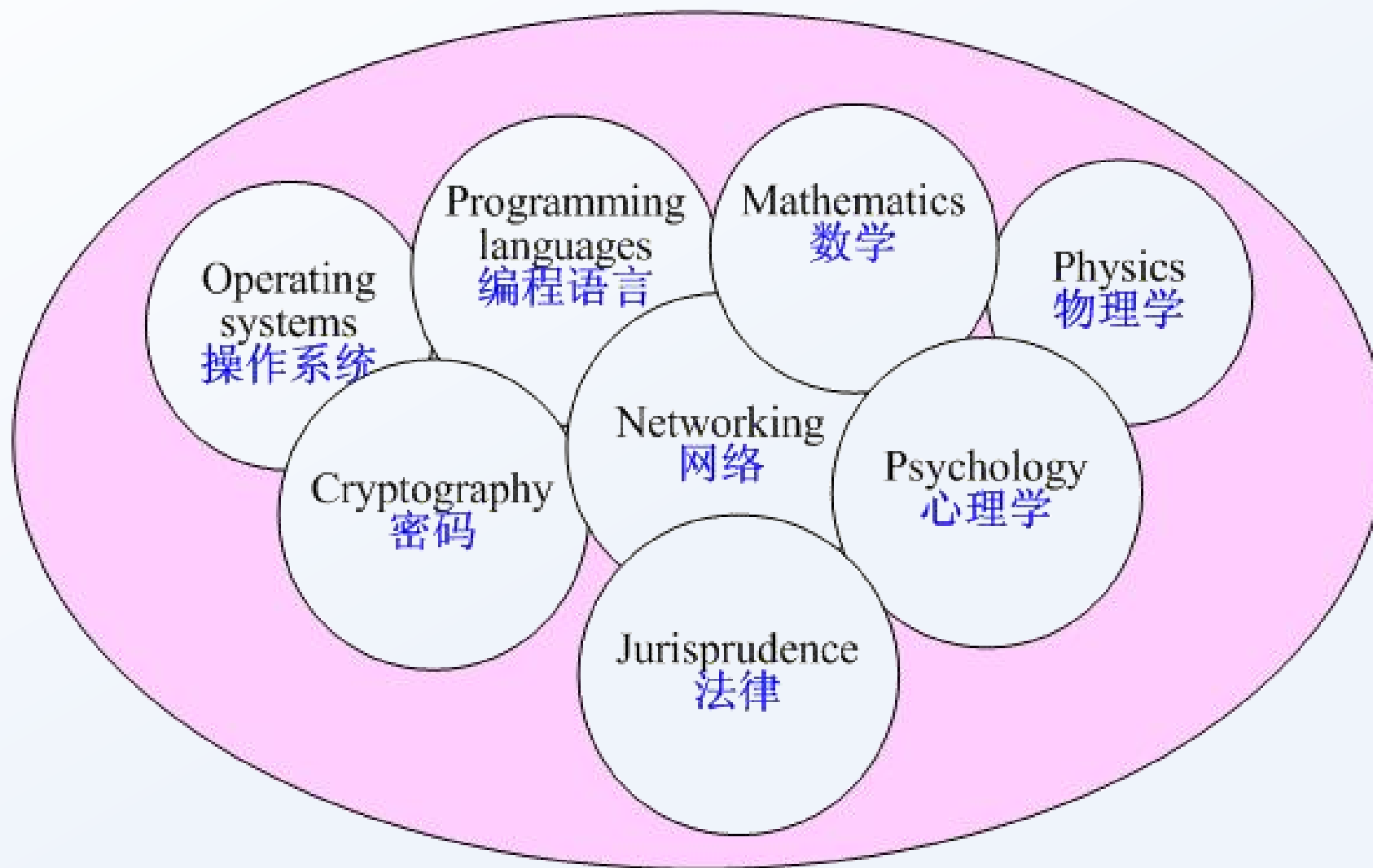
下载

有可用的可选更新

• 2020-适用于 Windows 10 Version 1909 的 08 累积更新, 适合基于 x64 的系统 (KB4566116)

[下载并安装](#)

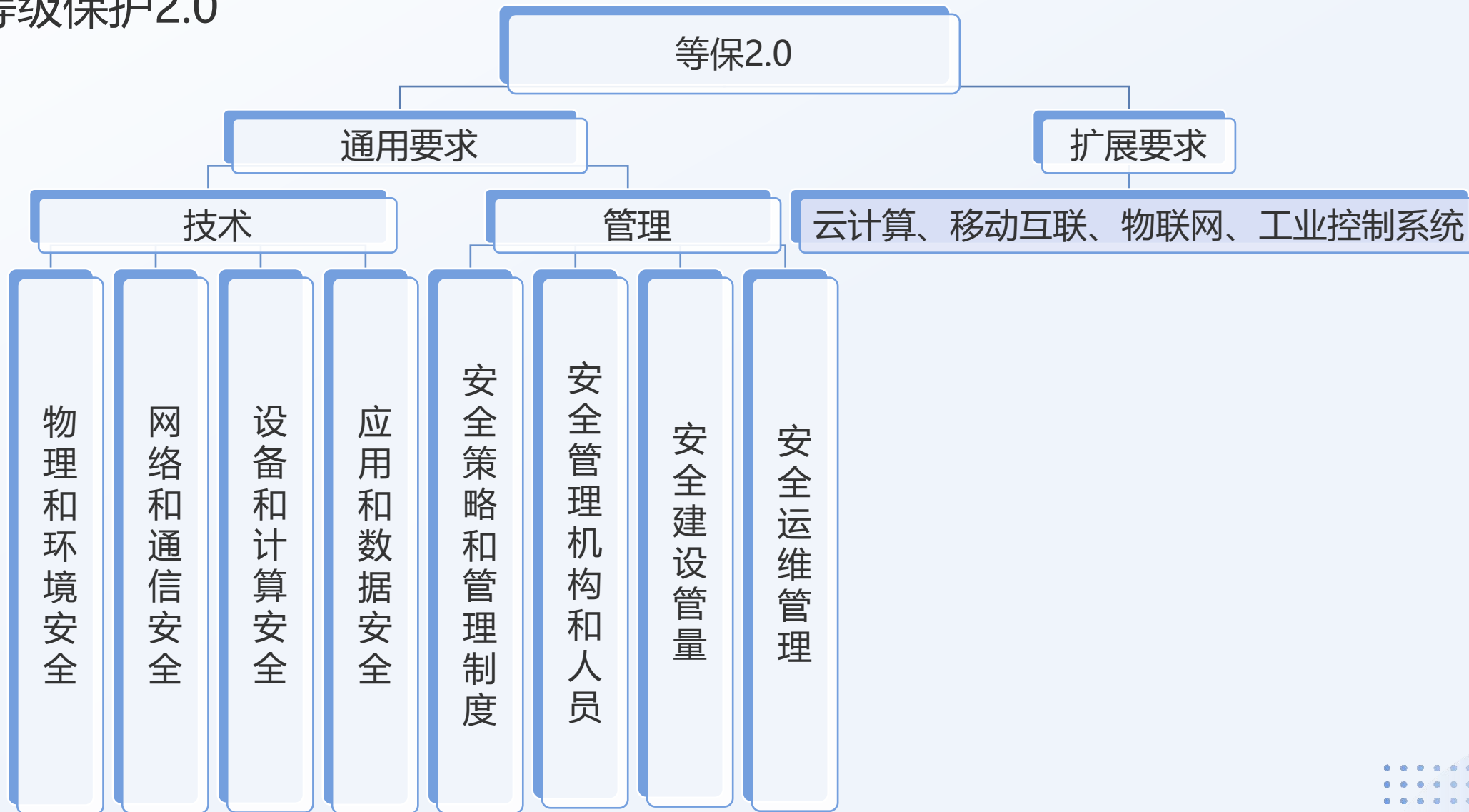
1.2 网络安全涉及的内容



1.2 网络安全涉及的内容



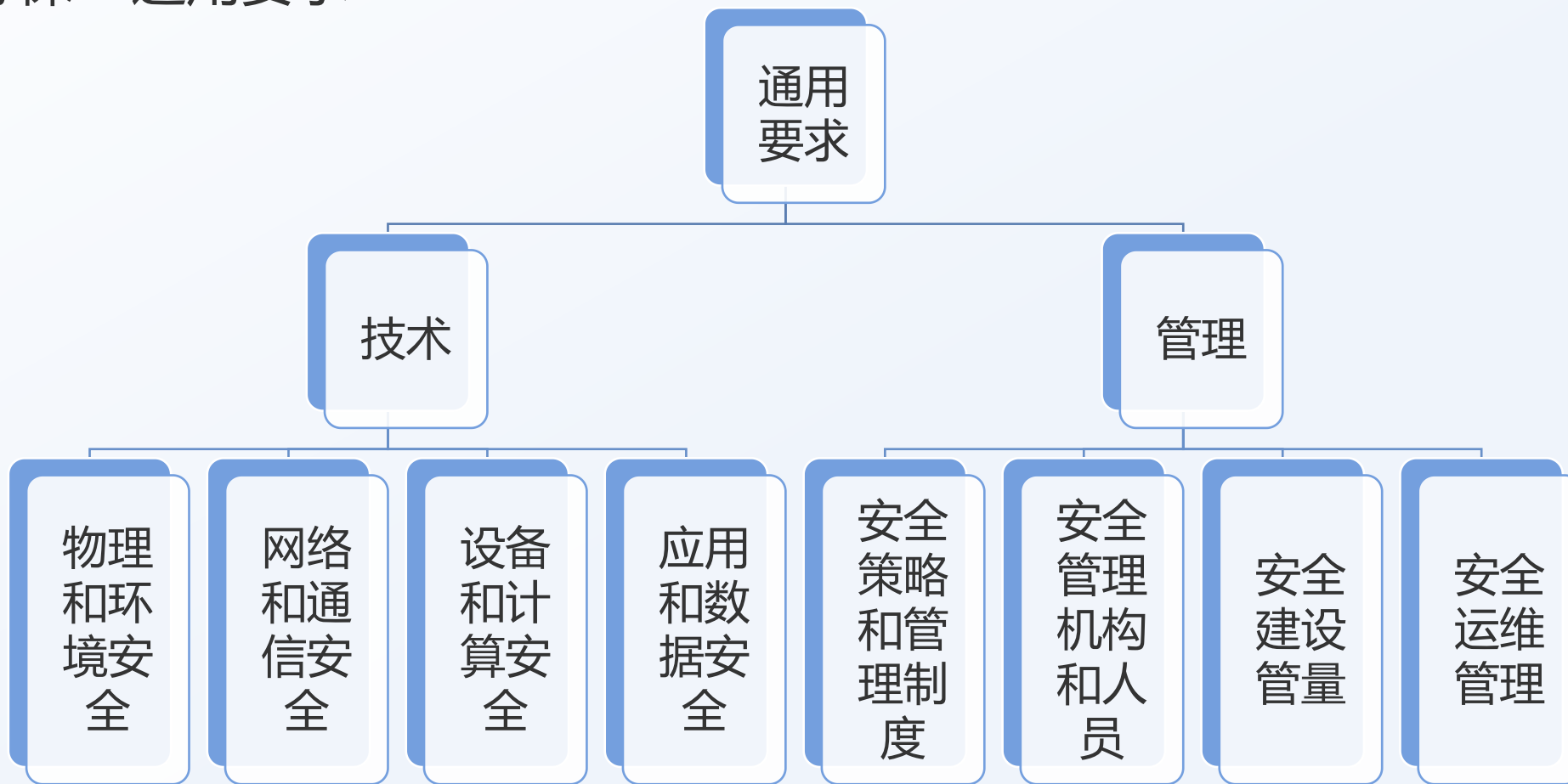
等级保护2.0



1.2 网络安全涉及的内容



等保—通用要求



1.2.1 物理和环境安全

物理安全控制


设备安全

主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

物理访问控制安全

建立访问控制机制，控制并限制所有对信息系计算、存储和通讯系统设施的物理访问。

环境安全

 为了确保计算机处理设施能正确、连续地运行，要考虑及防范以下威胁：火灾、电力供应中断、爆炸物、化学品等，还要考虑环境的温度和湿度是否适宜。



1.2.2

网络和通信安全

表1-3 网络和通信安全的组成

| 网络和通信安全 | 子项 | 举例 |
|---------|--------|-------------------------------------|
| | 网络架构 | 设计安全的拓扑、链路备份、IP划分等 |
| | 通信传输 | 防火墙等安全设备、数据加密（VPN等） |
| | 边界防护 | 对内部用户非授权联到外部网络的行为进行限制或检查；限制无线网络的使用等 |
| | 访问控制 | 访问控制功能的设备包括网闸、方后墙、路由器和三层路由交换机等 |
| | 入侵防范 | 入侵检测系统等 |
| | 恶意代码 | 关键网络节点处对恶意代码进行检测和防护 |
| | 垃圾邮件防范 | 关键网络节点处对垃圾邮件进行检测和防护 |
| | 安全审计 | 各系统配置日志，提供审计机制 |
| | 集中管控 | 集中监测、集中审计和集中管理 |



1.2.3 设备和计算安全

设备和计算安全，通常指设备、网络设备、安全设备和终端设备等节点设备自身的安全保护能力，一般通过启用防护软件的相关安全配置和策略来实现。这里包括各设备的操作系统本身的安全以及安全管理与配置内容。



1.2.4应用和数据安全

表1-4 应用和数据安全的组成

| 应用和数据安全 | 子项 | 举例 |
|---------|------|----------|
| | 应用安全 | 应用系统平台安全 |
| | | 应用软件安全 |
| | 数据安全 | 数据的保密性 |
| | | 数据的完整性 |
| | | 数据的备份和恢复 |

网络安全不是个目标，而是个过程。

