第四讲 操作系统安全

白杨 alicepub@163.com

操作系统安全

信息论 | 系统论 | ...

计算机理论 | 控制论

数学（代数、数论、概率统计、组合数学、博弈论）

网络空间安全基础理论

应用安全

系统安全

网络安全

密码学及应用

第四讲 操作系统安全

① 操作系统概述

② 操作系统的安全威胁

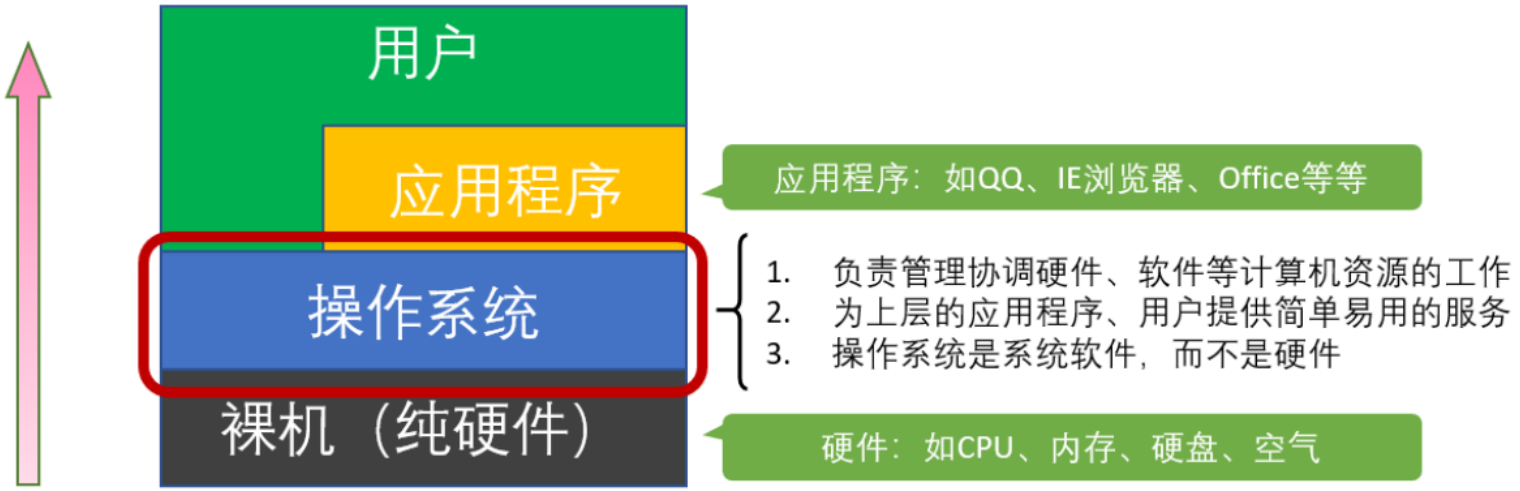
③ 操作系统典型安全事件

④ 操作系统安全需求与保护机制

⑤ 操作系统安全评估等级

操作系统的含义

操作系统定义：负责计算机系统的硬件资源管理，支撑和控制各种应用程序运行，为用户提供计算机系统管理接口。操作系统是构成网络信息系统的核心关键组件，其安全可靠程度决定了计算机系统的安全性和可靠性。



计算机系统的层次结构

操作系统的功能主要包括：

进程管理、内存管理、设备管理、文件管理、用户接口

操作系统的含义

操作系统的功能主要包括：

- **进程管理：**又称为处理器管理，主要负责对中央处理器（CPU）的时间进行合理分配、对处理器的运行进行有效的管理。
- **内存管理：**主要负责是对计算机内存空间进行合理分配、保护和扩充，用于解决多道进程共享内存资源时的冲突，并通过有效的管理方式提高计算机内存空间利用率。
- **设备管理：**根据一定的分配原则对计算机的硬件设备进行调度与分配，使设备与计算机能够并行工作，为用户提供良好的设备使用效果。
- **文件管理：**负责有效地管理计算机磁盘的存储空间，合理地组织和管理文件系统，为文件访问和文件保护提供更有效的方法及手段。
- **用户接口：**用户操作计算机的界面称为用户接口或用户界面，通过用户接口，用户只需通过简单操作，就可以实现复杂的计算或处理。用户接口主要分为命令行接口、图形界面接口和程序调用接口（Application Programming Interface，API）几种。

操作系统的典型产品

常见操作系统有：

- 微软公司Windows：Windows 95、Windows 98、Windows 2000、Windows XP、Windows 7、Windows 8、Windows 10、Windows 11等。
- 苹果公司macOS：使用BSD内核（基于UNIX）开发，1984年发布第一个版本，世界上第一个使用图形用户界面的操作系统，主要用于苹果电脑，最新版本为macOS 11
- 开源的Linux：Linux又称为GNU/Linux，1991年推出多进程多用户的操作系统，主要用于服务器环境，主要发行版有Ubuntu、Debian、Cent OS、RHEL、Arch Linux、Gentoo
- 移动操作系统有两类：谷歌的Android、苹果的iOS

第四讲 操作系统安全

① 操作系统概述

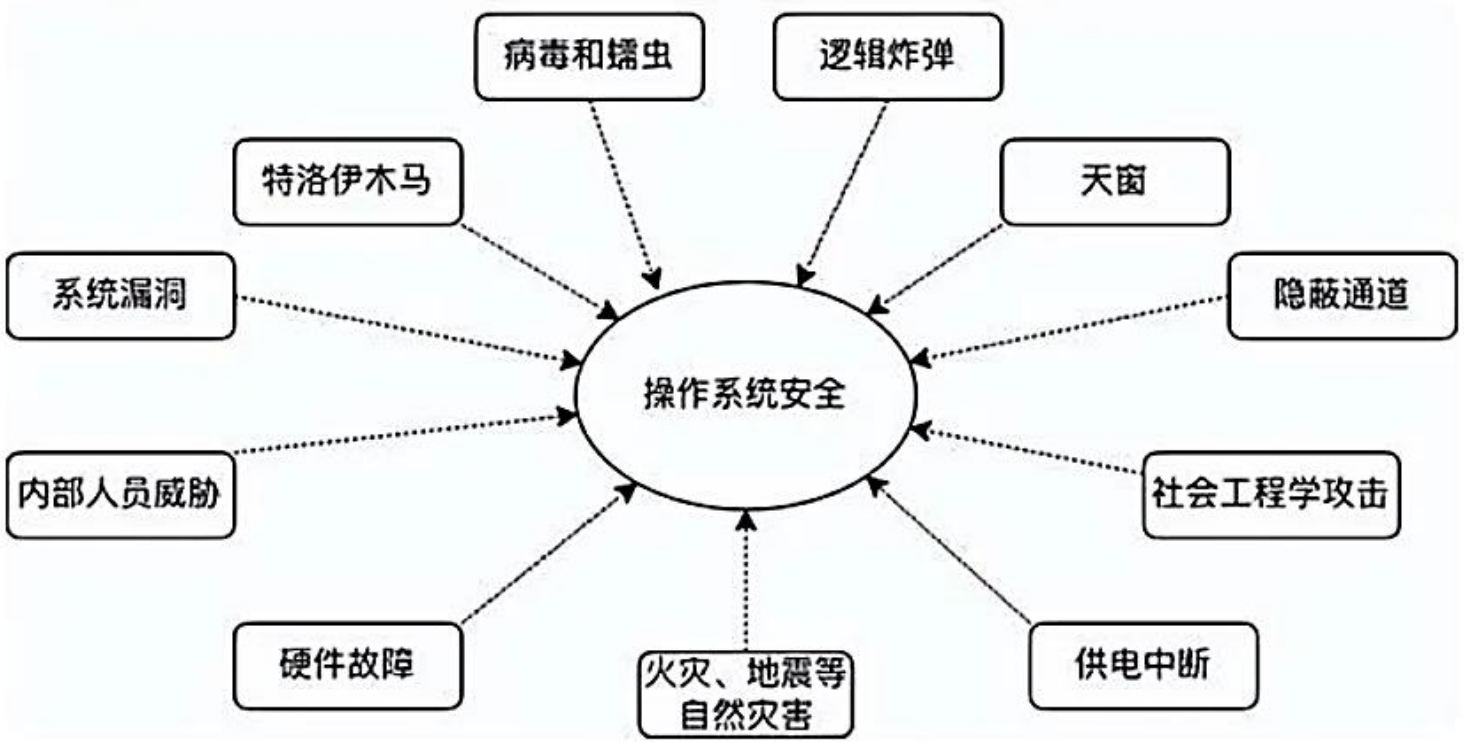
② 操作系统的安全威胁

③ 操作系统典型安全事件

④ 操作系统安全需求与保护机制

⑤ 操作系统安全评估等级

操作系统安全的威胁来源



其中系统漏洞、特洛伊木马、病毒、蠕虫、逻辑炸弹、天窗、隐蔽通道为技术方面的威胁；
内部人员威胁、硬件故障、供电中断、自然灾害、社会工程学为管理方面的威胁。

操作系统的技术安全威胁

后门(Trapdoor)

也称陷阱，某个正常程序的秘密入口，依靠某些特定输入串、某个特殊用户ID来激活

逻辑炸弹(Logic Bomb)

嵌入在正常程序中的一段恶意代码，在设定的条件满足时运行，如到达某个特定日期、增加或删除某个特定文件

特洛伊木马(Trojan Horses)

嵌入在正常程序中的一段恶意代码，表面上在执行合法任务，实际上却具有用户不曾料到的非法功能。主要在于削弱系统的安全控制机制，尤其是访问控制机制，实现非授权的网络访问的程序

计算机病毒(Viruses)

既具有自我复制能力，又必须寄生在其他程序(或文件)中的恶意代码，最大的特点是在人工干预下具备自我复制能力

蠕虫(Worms)

病毒的一种，具备自身复制使用的机制，它的传播不需要人工干预

隐蔽通道

可定义为系统中不受安全策略控制的、违反安全策略的信息泄露路径。 按信息传递的方式和方法区分,隐蔽通道分为隐蔽存储通道和隐蔽定时通道

第四讲 操作系统安全

① 操作系统概述

② 操作系统的安全威胁

③ 操作系统典型安全事件

④ 操作系统安全需求与保护机制

⑤ 操作系统安全评估等级

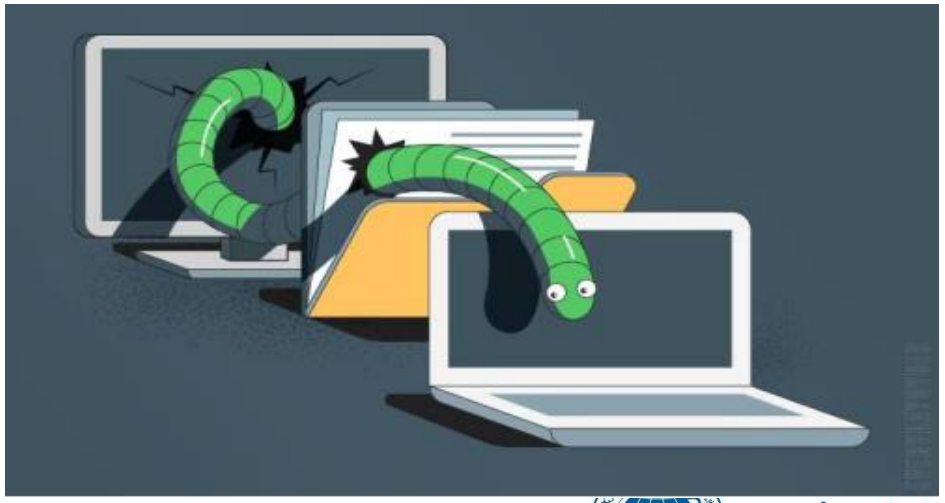
操作系统典型安全事件

莫里斯蠕虫

美国康乃尔大学一年级研究生罗伯特·莫里斯（现在是MIT的终身教授），莫里斯蠕虫发作于1988年11月2日，蠕虫用命令查询联机用户名单，然后破译用户口令，用Mail系统复制、传播蠕虫本身的源程序，再编译生成代码。

被感染的电脑“蠕虫”快速自我复制、挤占电脑系统里的硬盘空间和内存空间。12小时之内感染了6200台运行Unix操作系统的SUN工作站和VAX小型机，使之瘫痪或半瘫痪，造成了$10000000(1千万美元)的直接经济损失。

比事件影响更大、更深远的是：计算机病毒从此流行。



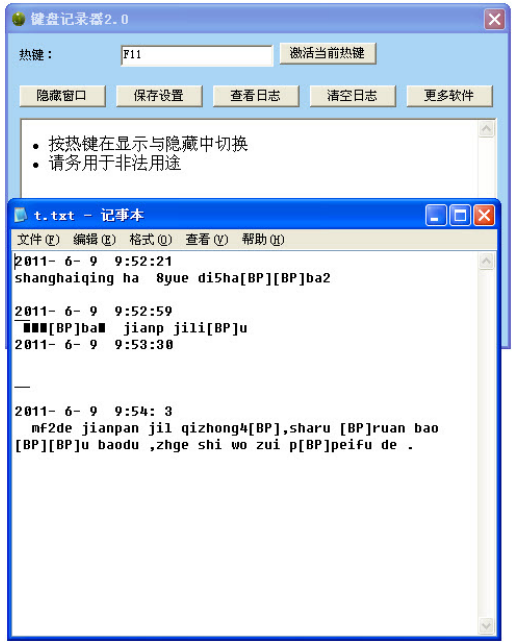
操作系统典型安全事件

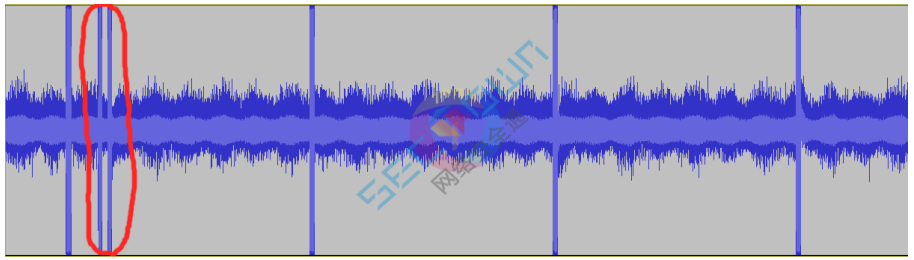
键盘木马

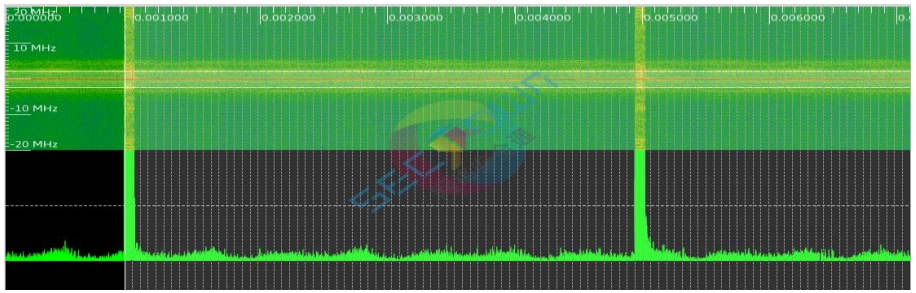
键盘程序被内置了键盘记录器的木马程序，会将键盘操作全部记录下来，存储或者发送。

为了对抗软件层面的攻击如键盘钩子，一些软件腾讯QQ，在用户输入密码等敏感信息时会用一个更底层的驱动程序截取键盘输入。但攻击者也可以通过驱动程序从操作系统内核中获取未经干扰的按键。

而通过硬件手段实现的键盘监听一般很难从软件层面发现。







操作系统典型安全事件

震荡波蠕虫（Sasser）

利用微软WindowsNT内核平台上的LSASS漏洞，随机的扫描其它网络中计算机的IP端口，然后进行传播。尽管该蠕虫在Windows 2000、Windows XP上发作，不会感染安装Windows 95/98/Me操作系统的计算机，但可以在这些操作系统上运行，而成为传播源。

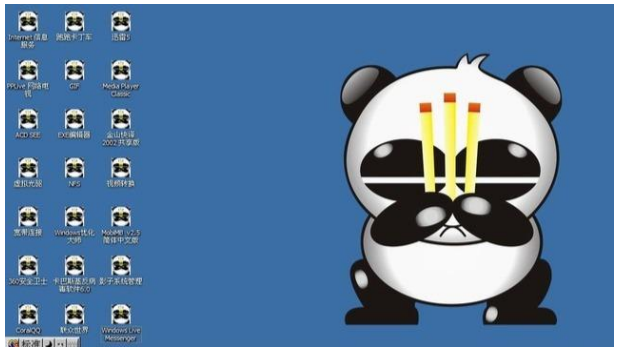
在该蠕虫传播的几天内，相继出现了B、C、D、E、F等变种蠕虫。其中的变种E和变种 F是编写者被逮捕之后出现的。

2004年5月7日，德国下萨克森州罗滕堡的18岁少年Sven Jaschan被捕，承认此前的蠕虫是他编写的。2005年7月8日，德国Verden市法院认定他制造震荡波蠕虫，四次改变量据和三次对计算机实施破坏有罪，判处21个月的缓刑，在缓刑期间必须完成30个小时的感化工作。。

操作系统典型安全事件

熊猫烧香

2006年10月16日由25岁的中国湖北武汉新洲区人李俊编写，2007年1月初肆虐中国大陆网络，2007年2月12日，湖北省公安厅宣布，李俊以及其同伙共8人落网。



1.病毒会删除扩展名为gho的文件，使用户无法使用ghost软件恢复操作系统。

2.感染系统可执行文件，如EXE,SCR,PIF,COM 文件，将感染目标文件和病毒溶合成一个文件（被感染文件贴在病毒文件尾部）

3.感染htm,html,asp,php,jsp,aspx脚本类文件，添加病毒网址，导致用户一打开这些网页文件，IE就会自动连接到指定的病毒网址中下载病毒。一些网站编辑人员的电脑如果被该病毒感染，上传网页到网站后，就会导致用户浏览这些网站时也被病毒感染。

在硬盘各个分区下生成文件autorun.inf和setup.exe，可以通过U盘和移动硬盘等方式进行传播，并且利用Windows系统的自动播放功能来运行，搜索硬盘中的.exe可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案。“熊猫烧香”还可以通过共享文件夹、用户简单密码等多种方式进行传播。致使“熊猫烧香”病毒的感染范围非常广，中毒企业和政府机构已经超过千家，其中不乏金融、税务、能源等关系到国计民生的重要单位。

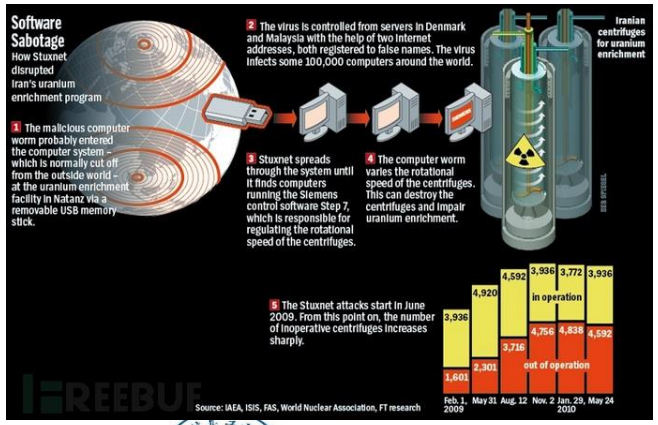
操作系统典型安全事件

震网病毒，Stuxnet，又被称为超级工厂病毒

是世界上首个专门针对工业控制系统编写的破坏性病毒，能够利用对windows系统和西门子SIMATIC WinCC系统的7个漏洞进行攻击。特别是针对西门子公司的SIMATIC WinCC监控与数据采集（SCADA）系统进行攻击。病毒向可编程逻辑控制器写入代码并将代码隐藏。该病毒可能已感染并破坏了伊朗纳坦兹的核设施（坏掉了1000台离心机），并最终使伊朗的布什尔核电站推迟启动。2010年6月首次被白俄罗斯安全公司VirusBlokAda发现，它的传播从2009年6月或更早开始，2010-09-25，进入中国。

俄罗斯卡巴斯基实验室发布了一个声明“是一种十分有效并且可怕的网络武器原型，这种网络武器将导致世界上新的军备竞赛，一场网络军备竞赛时代的到来。除非有国家和政府的支持和协助，否则很难发动如此规模的攻击。”

传播途径：该病毒主要通过U盘和局域网进行传播。

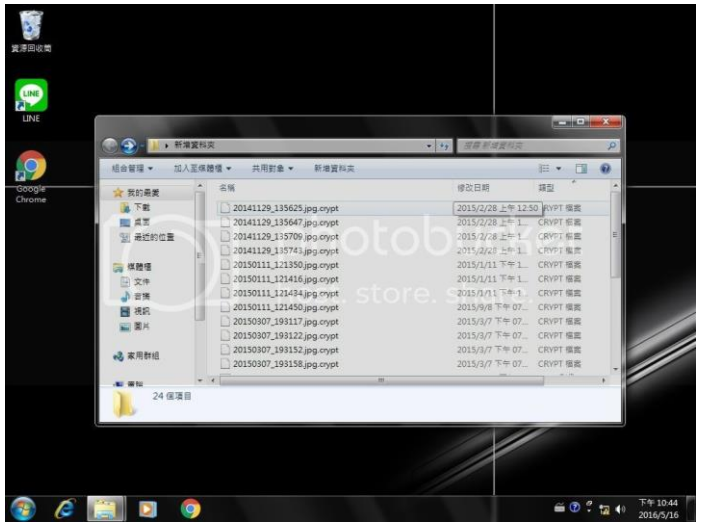


操作系统典型安全事件

勒索软件

CryptoLocker于2013年下半年出现的特洛伊木马，以勒索软件的形式出现的恶意软件，以Windows操作系统为主要攻击目标，所派生的变种也向Linux等操作系统及特定厂牌的网络存储设备（NAS）攻击。

CryptoLocker会伪装成一个合法的电子邮件附件或.exe格式文件。如果被激活，该恶意软件就会使用RSA、AES等算法加密本地与内部网的特定类型文件。而私人密钥则把持在恶意软件所控制的服务器上。该蠕虫会显示一则消息，表示如果在规定的期限进行付款（经由比特币或其他储值管道），就能够解密这些文件，否则私人密钥将会被销毁，再也不能打开这些文件。



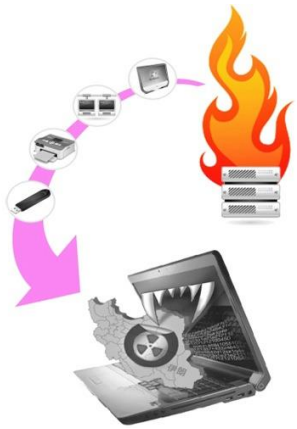
操作系统典型安全事件

火焰病毒

火焰病毒，2012年5月被发现的恶意软件，利用微软公司Windows操作系统的两处漏洞侵入电脑并注入程序。大约从2010年开始散播，其所包含的代码量约是之前发现的震网病毒（Stuxnet）或毒区病毒（Duqu）的20倍，被称为有史以来最复杂的恶意软件，在中东大范围传播。火焰病毒收集个人信息并上传到网络，录音、截取屏幕画面、侵入邻近的蓝牙设备。

伊朗方面于2012年4月时，称该病毒被其创造者命名为Wiper 。而卡巴斯基则说它和Wiper没有什么关系。尽管以色列副部长摩西的某段讲话似乎暗示了以色列是始作俑者，但目前以色列在受害数量上仅次于伊朗的189起，为89。

有报导声称该恶意软件由美国国家安全局和以色列合作研发。类似震网病毒，可能都在Olympic Games计划下开发出来。美国和以色列都正式否认与此病毒有关。



操作系统典型安全事件

手机操作系统系统漏洞：

iPhone曝“末日漏洞”，沦为间谍软件的监视工具。据 Citizen Lab 和微软的研究人员于2023年4月11日公开的报告，一家以色列间谍公司开发出的间谍应用 Reign被用来感染iPhone设备，对多国记者、不同党派要员和非政府组织工作人员进行监视。报告披露了这家名为QuaDream的间谍公司开发的这款间谍软件能够录制音频、拍照、跟踪位置和窃取密码，至少有10个国家或地区的政府曾进行采购。

2023年3月28 日，苹果发布了 iOS / iPadOS 16.4 正式版和 macOS 13.3 系统更新，引入了安全补丁，修复了 30 多处漏洞。苹果官方更新日志中表示：本次 iOS 16.4、macOS Ventura 13.3、watchOS 9.4 和 tvOS 16.4 更新修复了数十个可能被黑客利用的安全漏洞。苹果还修复了内核方面的漏洞，允许黑客在用户不知情的情况下执行任意代码。


iOS 15.7.5 和 iPadOS 15.7.5

2023 年 4 月 10 日发布

IOSurface加速器

适用于：iPhone 6s (所有型号)、iPhone 7 (所有型号)、iPhone SE (第 1 代)、iPad Air 2、iPad mini (第 4 代) 和 iPod touch (第 7 代)

影响：应用程序或许能够使用内核权限执行任意代码。Apple 获悉一份报告称此问题可能已被积极利用。

描述：越界写入问题已通过改进输入验证得到解决。

CVE-2023-28206：Google 威胁分析小组的 Clément Lecigne 和国际特赦组织安全实验室的 Donncha Ó Cearbhaill

网络套件

适用于：iPhone 6s (所有型号)、iPhone 7 (所有型号)、iPhone SE (第 1 代)、iPad Air 2、iPad mini (第 4 代) 和 iPod touch (第 7 代)

影响：处理恶意制作的网页内容可能会导致任意代码执行。Apple 获悉一份报告称此问题可能已被积极利用。

描述：已通过改进内存管理解决释放后使用问题。

WebKit Bugzilla：254797

CVE-2023-28205：谷歌威胁分析小组的 Clément Lecigne 和国际特赦组织安全实验室的 Donncha Ó Cearbhaill

第四讲 操作系统安全

① 操作系统概述

② 操作系统的安全威胁

③ 操作系统典型安全事件

④ 操作系统安全需求与保护机制

⑤ 操作系统安全评估等级

操作系统安全需求

操作系统的安全需求：

标识和鉴别：能够唯一标识系统中的用户，并进行身份真实性鉴别

访问控制：通过资源访问控制，防止用户对计算机资源的非法窃取、篡改、破坏

系统资源安全：保护系统中信息及数据的完整性、保密性、可用性

网络安全：通过网络访问控制，确保网络通信数据安全、网络服务的可用性

抗攻击：具有系统运行监督机制，防御恶意代码攻击

自身安全：确保系统安全和完整性，具有可信恢复能力

操作系统安全常用保护机制—标识与鉴别

标识和鉴别：能够唯一标识系统中的用户，并进行身份真实性鉴别

标识与鉴别是涉及系统和用户的一个过程。标识就是系统要标识用户的身份，并为每个用户取一个系统可识别的用户标识符，用户**标识符唯一且不可伪造**，防止用户冒充行为。鉴别是用户标识符与用户联系的过程。鉴别过程主要用于识别用户的真实身份。

在操作系统中，用户登录的过程就属于系统对用户合法性的鉴别。可以从以下几个方面来加强鉴别安全：

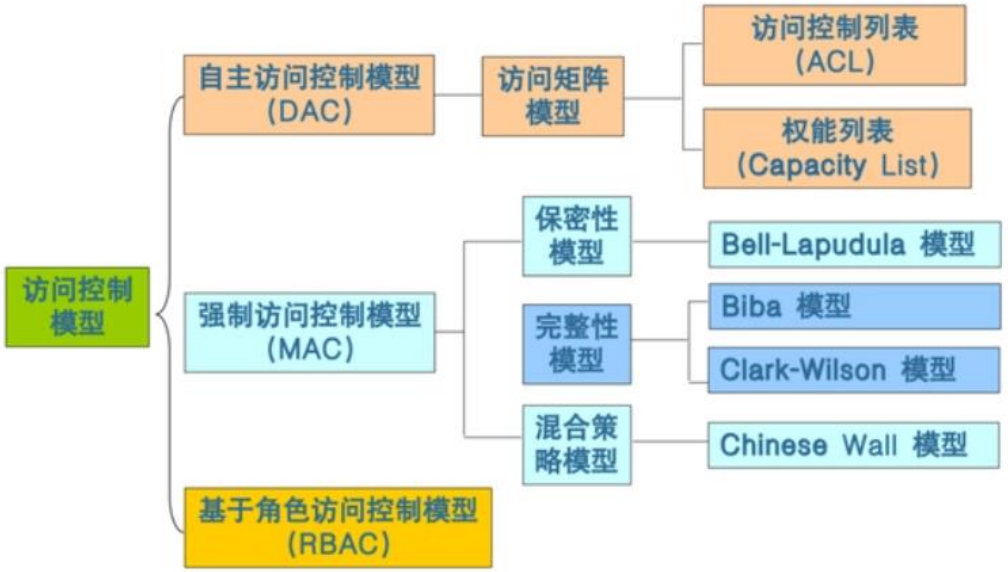
- 对于采用静态口令认证技术的设备，**帐户口令的生存期不长于 90 天**。
- 对于采用静态口令认证技术的设备，**口令长度至少12 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类**。
- 配置当用户连续认证**失败次数超过 5 次**，锁定该用户使用的帐号。
- 用户远程登录**禁用root用户**。
- 对于安全等级要求高的设备，采用**静态口令+数字证书或生物识别的双因子认证**。

操作系统安全常用保护机制—访问控制

访问控制：访问控制是为用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理，防止对信息的非授权篡改和滥用。（例如：Linux文件访问控制）

自主访问控制：是由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体，这种控制方式是基于用户的，具有很高的灵活性。需要注意的是，在配置客体的权限时，要根据最小权限原则对客体配置自主访问控制权限。

强制访问控制：系统中的主体和客体都被赋予了相应的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体。安全属性是不能改变的，它由系统管理人员(如安全管理员)或由操作系统自动地按照严格的规则来设置，不像访问控制表那样由用户或他们的程序直接或间接地修改。



操作系统安全常用保护机制—最小权限原则

最小权限原则： 是指仅仅给予人员、程序系统**最小**能完成其功能的权限。在操作系统运维工作中，最小化权限原则应用的一些例子包括：

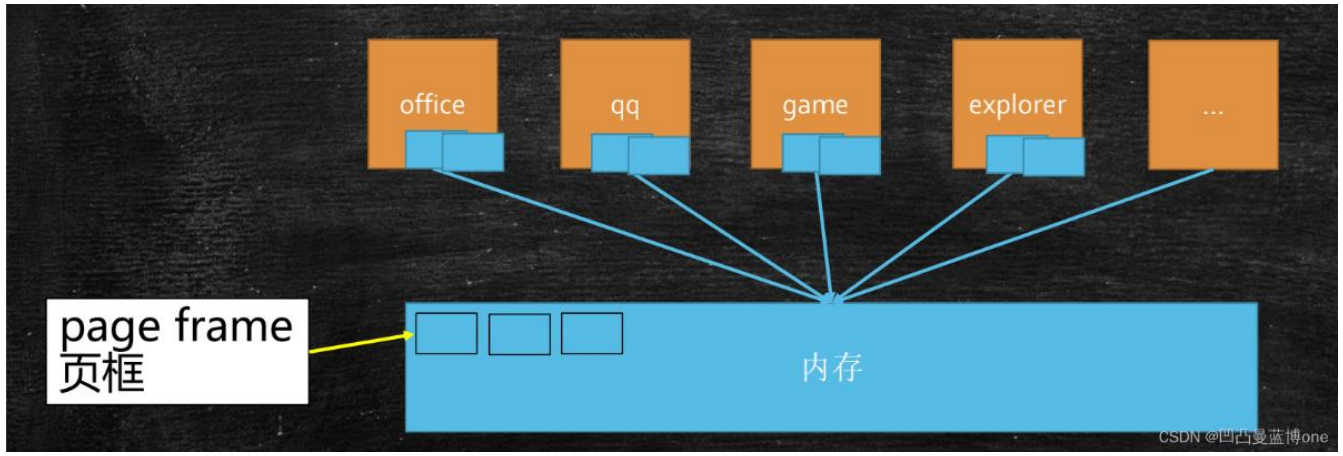
- 服务器网络访问权限控制。如当信息系统的后端服务不需要被外部访问时，禁止对其分配公网IP或开放端口。
- 使用普通用户运行应用程序。例如在Linux环境中，Mysql、Httpd、Nginx等对外提供服务的程序都应该使用普通用户来运行，以此来有效降低应用程序漏洞带来的安全风险。
- 为应用程序创建隔离环境。例如通过chroot将程序运行环境切换到指定目录。
- 关闭不必要的系统服务。

操作系统安全常用保护机制——进程隔离与内存保护

进程隔离与内存保护：当前的计算机系统早已完全实现了多任务模式，即多项不同的任务同时在一台计算机中运行。当计算机同时执行多项任务时，为了避免不同任务间的互相影响，操作系统提供了进程隔离与内存保护机制。

为了实现进程隔离与内存保护的机制，计算机操作系统中加入了**内存管理单元（MemoryManagement Unit，MMU）**模块，当程序在计算机中运行时由MMU模块负责进程分配运行所需的内存空间，进程隔离与内存保护机制为每个进程提供互相独立的运行空间，该机制通过禁止进程读写其他进程以及系统进程的内存空间来实现隔离，并通过一些列复杂的机制实现隔离环境下的**进程间通信(IPC)**机制与进程间资源共享机制。

进程隔离与内存保护机制为操作系统的安全性做出了重要贡献



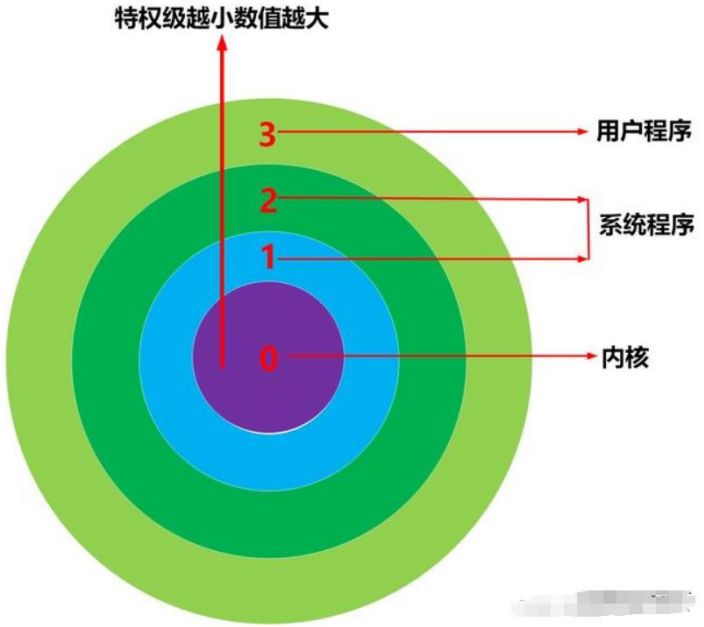
操作系统安全常用保护机制—运行保护

运行模式保护：

为了安全性的目的，现代CPU的运行模式通常分为**内核模式**与**用户模式**两种运行模式：

- 内核模式，也称为特权模式，在Intel x86 系列中，称为核心层(Ring 0)。
- 用户模式，也称为非特权模式，或者用户层(Ring 3)。

如果CPU 处于特权模式，那么将允许执行一些仅在特权模式下许可的特殊指令和操作。操作系统通常运行在特权模式或者称为内核模式下，其他应用程序则运行在普通模式，即用户模式下。CPU运行模式的区分起到了保护操作系统的运行不受其他应用程序干扰和破坏的作用，大大提升了操作系统的安全性。



操作系统安全常用保护机制—其他

文件系统加密：为了防止因信息载体落入他人手中而导致的信息泄露问题，可以采取对信息进行加密的措施。在操作系统中实现信息加密的方法很多，可以对单个文件进行加密，也可以对整个磁盘进行加密。（例如：NTFS加密）

白名单机制：网络访问中，白名单机制明确定义了什么是被允许的，除此之外的情况全部拒绝。白名单机制和黑名单机制相对，黑名单机制明确定义了什么是不被允许的。

安全审计：安全审计就是对操作系统中涉及安全事件的活动进行记录、检查、审核或追溯。它的主要目的就是检测非法用户对计算机系统的入侵，显示合法用户的误操作，并能及时发出安全警告以便让管理员对入侵事件进行快速响应。（审计权限分割）

第四讲 操作系统安全

① 操作系统概述

② 操作系统的安全威胁

③ 操作系统典型安全事件

④ 操作系统安全需求与保护机制

⑤ 操作系统安全评估等级

操作系统安全评估等级

操作系统安全：满足安全策略要求，具有相应的安全机制及安全功能，符合特定的安全标准，在一定约束条件下，能够抵御常见的网络安全威胁，保障自身的安全运行及资源安全。

国家标准《信息安全技术 操作系统安全技术要求（GB/T 20272-2019）》将操作系统分成五个安全等级：

用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级

可信计算机系统评估标准(TCSEC)

美国国防部把计算机系统的安全从低到高分为4等8级：

D等（最低保护等）：D1（安全保护欠缺级）

C等（自主保护等）：C1（自主安全保护级）、C2（受控安全保护级）

B等（强制保护等）：B1（标记安全保护级）、B2（结构化保护级）、B3（安全域级）

A等（验证保护等）： A1级、A2级

Windows NT 4.0 安全级基本达到了 C2

小结：操作系统安全的病毒防范

- **修补操作系统以及其捆绑的软件的漏洞**

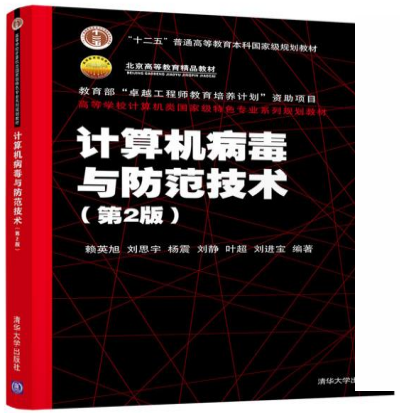
  以操作系统Windows为例，用系统的“自动更新”程序下载补丁进行安装。设置一个比较强的系统密码，关闭系统默认网络共享，防止局域网入侵或弱口令蠕虫传播。定期检查系统配置实用程序启动选项卡情况，并对不明的Windows服务予以停止。

- **安装并及时更新杀毒软件与防火墙产品**

  保持最新病毒库以便能够查出最新的病毒，如一些反病毒软件的升级服务器每小时就有新病毒库包可供用户更新。而在防火墙的使用中应注意到禁止来路不明的软件访问网络。

- **不要点来路不明连接以及运行不明程序**

  通过电子邮件或即时通讯软件发过来的来路不明的连接，用户访问这些网站后不用下载直接就可能会中更多的病毒。不要点击，点击后病毒就在系统中运行了。



THE END