第3章 操作系统安全

3.1 国际安全评价标准的发展及其联系


视频讲解

计算机系统安全评价标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法、执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评价事关国家的安全利益，许多国家都在充分借鉴国际标准的前提下，积极制定本国的计算机安全评价认证标准。

第1个有关信息技术安全评价的标准诞生于20世纪80年代的美国，就是著名的可信计算机系统评价准则(Trusted Computer System Evaluation Criteria，TCSEC)，又称为橘皮书。该准则对计算机操作系统的安全性规定了不同的等级。从20世纪90年代开始，一些国家和国际组织相继提出了新的安全评价准则。1991年，欧共体发布了信息技术安全评价准则(Information Technology Security Evaluation Criteria，ITSEC)。1993年，加拿大发布了加拿大可信计算机产品评价准则(Canadian Trusted Computer Product Evaluation Criteria，CTCPEC)，CTCPEC综合TCSEC和ITSEC两个准则的优点。同年，美国在对TCSEC进行修改补充并吸收ITSEC优点的基础上发布了信息技术安全评价联邦准则(Federal Criteria，FC)，如图3.1所示。

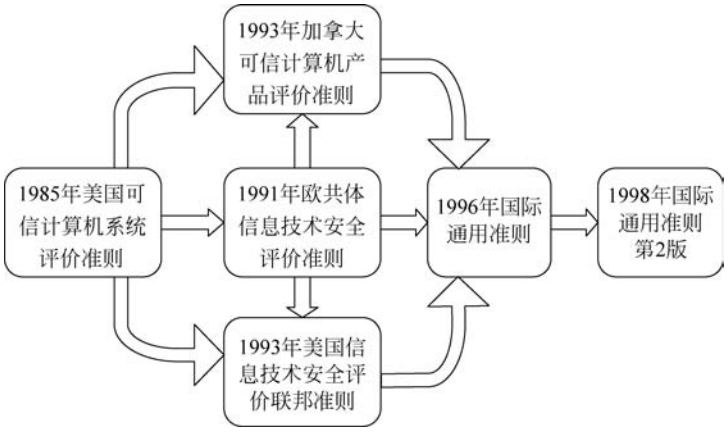

图3.1 安全评价标准的发展

1996年6月，上述国家共同起草了一份通用准则(Common Criteria，CC)，并将CC推广为国际标准。CC发布的目的是建立一个各国都能接受的通用的安全评价准则，国家与

国家之间可以通过签订互认协议决定相互接受的认可级别,这样能使基础性安全产品在通过CC准则评价并得到许可后进入国际市场时不需要再作评价。此外,国际标准化组织和国际电工委也已经制定了上百项安全标准,其中包括专门针对银行业务制定的信息安全标准。国际电信联盟和欧洲计算机制造商协会也推出了许多安全标准。

3.1.1 计算机安全评价标准

计算机安全评价标准(TCSEC)是计算机系统安全评估的第1个正式标准,具有划时代的意义。该准则于1970年由美国国防科学委员会提出,并于1985年12月由美国国防部公布。TCSEC最初只是军用标准,后来延至民用领域。TCSEC将计算机系统的安全划分为4个等级、7个级别。

1. D类安全等级

D类安全等级只包括D1一个级别。D1的安全等级最低,D1系统只为文件和用户提供安全保护。D1系统最普通的形式是本地操作系统,或者是一个完全没有保护的网络。

2. C类安全等级

C类安全等级能够提供审慎的保护,并为用户的行动和责任提供审计能力。C类安全等级可划分为C1和C2两个级别。C1系统的可信任运算基础体制,通过将用户和数据分开来达到安全的目的。在C1系统中,所有用户以同样的灵敏度处理数据,即用户认为C1系统中的所有文档都具有相同的机密性。C2系统比C1系统加强了可调的审慎控制。在连接到网络上时,C2系统的用户分别对各自的行为负责。C2系统通过登录过程、安全事件和资源隔离增强这种控制。C2系统具有C1系统中所有的安全性特征。

3. B类安全等级

B类安全等级可分为B1、B2和B3级别。B类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连,系统就不会让用户存取对象。

B1系统满足下列要求:系统对网络控制下的每个对象都进行灵敏度标记,系统使用灵敏度标记作为所有强迫访问控制的基础。系统在把导入的、非标记的对象放入系统前标记。灵敏度标记必须准确地表示其所联系的对象的安全级别。当系统管理员创建系统或增加新的通信通道或I/O设备时,管理员必须指定每个通信通道和输入/输出(Input/Output,I/O)设备是单级还是多级,并且管理员只能手工改变指定。单级设备并不保持传输信息的灵敏度级别,所有直接面向用户位置的输出(无论是虚拟的还是物理的)都必须产生标记以指示关于输出对象的灵敏度,系统必须使用用户的口令或证明决定用户的安全访问级别,系统必须通过审计记录未授权访问的企图。

B2系统必须满足B1系统的所有要求。另外,B2系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2系统必须满足下列要求:系统必须立即通知系统中的每个用户所有与之相关的网络连接的改变。只有用户能够在可信任通信路径中进行初始化通信,可信任运算基础体制能够支持独立的操作者和管理员。

B3系统必须符合B2系统的所有安全需求。B3系统具有很强的监视委托管理访问能力和抗干扰能力。B3系统必须设有安全管理员。B3系统应满足以下要求:除了控制对个别对象的访问外,B3系统必须产生一个可读的安全列表,每个被命名的对象提供对该对象没有访问权的用户列表说明,B3系统在进行任何操作前要求用户进行身份验证。B3系统验证每个

用户，同时还会发送一个取消访问的审计跟踪消息。设计者必须正确区分可信任的通信路径和其他路径，可信任的通信基础体制为每个被命名的对象建立安全审计跟踪，可信任的运算基础体制支持独立的安全管理。

4. A类安全等级

A系统的安全级别最高。目前，A类安全等级只包含A1一个安全类别。A1级别与B3级别相似，对系统的结构和策略不作特别要求。A1系统的显著特征是系统的设计者必须按照一个正式的设计规范分析系统。对系统分析后，设计者必须运用核对技术确保系统符合设计规范。A1系统必须满足下列要求：系统管理员必须从开发者那里接收一个安全策略的正式模型，所有的安装操作都必须由系统管理员进行，系统管理员进行的每步安装操作都必须有正式文档。

3.1.2 欧洲安全评价标准

ITSEC是欧洲多国安全评价方法的综合产物，应用领域为军事、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则分为F1～F10共10级。F1～F5级对应于TCSEC的D～A类。F6～F10级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性及机密性和完整性的网络安全。评估准则分为6级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应、设计与源码在形式上一致。

ITSEC定义了从E0级(不满足品质)～E6级(形式化验证)的7个安全等级，对于每个系统，安全功能可分别定义。这7个安全等级分别如下。

(1) E0级：该级别表示不充分的安全保证。

(2) E1级：该级别必须有一个安全目标和一个对产品或系统的体系结构设计的非形式化的描述，还需要有功能测试，以表明是否达到安全目标。

(3) E2级：除了E1级的要求外，还必须对详细的设计有非形式化描述。另外，功能测试的证据必须被评估，必须有配置控制系统和认可的分配过程。

(4) E3级：除了E2级的要求外，不仅要评估与安全机制相对应的源代码和硬件设计图，还要评估测试这些机制的证据。

(5) E4级：除了E3级的要求外，必须有支持安全目标的安全策略的基本形式模型。

(6) E5级：除了E4级的要求外，在详细的设计和源代码或硬件设计图之间有紧密的对应关系。

(7) E6级：除了E5级的要求外，必须正式说明安全加强功能和体系结构设计，使其与安全策略的基本形式模型一致。

3.1.3 加拿大评价标准

加拿大的CTCPEC专门针对政府需求而设计。与ITSEC类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为4大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类以表示安全性上的差别，分为0～5级。

3.1.4 美国联邦准则

FC是对TCSEC的升级,并引入了保护轮廓(Protection Profile,PP)的概念。每个轮廓都包括功能、开发保证和评价3部分。FC充分吸取了ITSEC和CTCPEC的优点,在美国的政府、民间和商业领域得到广泛应用。但FC有很多缺陷,它是一个过渡标准,后来结合ITSEC发展为国际通用准则。

3.1.5 国际通用准则

CC是国际标准化组织统一现有多种准则的结果,是目前最全面的评价准则。1996年6月,CC第1版发布;1998年5月,CC第2版发布;1999年10月,CC v2.1发布,并且成为ISO标准。CC的主要思想和框架都取自ITSEC和FC,并充分突出了"保护轮廓"概念。CC将评估过程划分为功能和保证两部分,评估等级分为eal1～eal7共7个等级。每级均需评估7个功能类,分别为配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试、脆弱性评估。

视频讲解

3.2 我国安全标准简介

我国信息安全研究经历了通信保密和计算机数据保护两个发展阶段,正在进入网络信息安全的研究阶段。通过学习、吸收、消化TCSEC的原则,进行了安全操作系统、多级安全数据库的研制,但由于系统安全内核受控于人,以及国外产品的不断更新升级,基于具体产品的增强安全功能的成果,难以保证没有漏洞,难以得到推广应用。在学习借鉴国外技术的基础上,国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是,这些产品安全技术的完善性、规范化、实用性还存在许多不足,特别是在多平台的兼容性以及安全工具的协作配合和互动性方面存在很大距离,理论基础和自主的技术手段也需要发展和强化。

以前,国内主要是等同采用国际标准。现在,由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准GB 17859—1999《计算机信息系统安全保护等级划分准则》已经正式颁布并使用了。该准则将信息系统安全分为5个等级,分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等,这些指标涵盖了不同级别的安全要求。

3.2.1 用户自主保护级

用户自主保护级的可信计算基通过隔离用户与数据,使用户具备自主安全保护的能力,具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段,保护用户和用户组信息,避免其他用户对数据的非法读写与破坏,具体表现在以下几方面。

(1) 可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(如访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享,阻止非授权用户读取敏感信息。

(2) 可信计算基初始执行时,首先要求用户标识自己的身份,并使用保护机制(如口令)鉴别用户的身份,阻止非授权用户访问用户身份鉴别数据。

(3) 可信计算基通过自主完整性策略,阻止非授权用户修改或破坏敏感信息。

3.2.2 系统审计保护级

与用户自主保护级相比,系统审计保护级的可信计算基实施了粒度更细的自主访问控制,通过登录规程、审计安全性相关事件和隔离资源,使用户对自己的行为负责。它增加了客体重用和安全审计方面的内容,并进一步增强了自主访问控制和身份鉴别机制,具体表现在以下几方面。

(1) 自主访问控制机制根据用户指定方式或默认方式阻止非授权用户访问客体。访问控制的粒度是单个用户。控制访问权限扩散,没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 通过为用户提供唯一标识,可信计算基能够使用户对自己的行为负责。可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(3) 在可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

(4) 可信计算基能创建和维护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。可信计算基能记录如下事件:使用身份鉴别机制;将客体引入用户地址空间(如打开文件、程序初始化);删除客体;由操作员、系统管理员或(和)系统安全管理员实施的动作,以及其他与系统安全有关的事件。对于每个事件,其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件,审计记录包含的来源(如终端标识符);对于客体引入用户地址空间的事件和客体删除事件,审计记录包含客体名。对不能由可信计算基独立分辨的审计事件,审计机制提供审计记录接口,可由授权主体调用。这些审计记录区别于可信计算基独立分辨的审计记录。

3.2.3 安全标记保护级

安全标记保护级的可信计算基具有系统审计保护级的所有功能。此外,还提供有关安全策略模型、数据标记及主体对客体强制访问控制的非形式化描述;具有准确地标记输出信息的能力;消除通过测试发现的任何错误。它增加了强制访问控制机制,具体表现在以下几方面。

(1) 可信计算基对所有主体及其所控制的客体(如进程、文件、段、设备)实施强制访问控制,为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。可信计算基支持两种或两种以上成分组成的安全级。可信计算基控制的所有主体对客体的访问应满足:仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别,主体才能读客体;仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的非等级类别,主体才能写客体。可信计算基使用身份和鉴别数据,鉴别用户的身份,并保证用户创建的可信计算基外部主体的安全

级和授权该用户的安全级。

(2) 可信计算基应维护与主体及其控制的存储客体(如进程、文件、段、设备)相关的敏感标记,这些标记是实施强制访问的基础。为了输入未加安全标记的数据,可信计算基向授权用户要求并接受这些数据的安全级别,且可由可信计算基审计。

(3) 在审计记录的内容中,对于客体引入用户地址空间的事件及客体删除事件,审计记录包含客体名及客体的安全级别。此外,可信计算基具有审计更改可读输出记号的能力。

(4) 在网络环境中,使用完整性敏感标记确认信息在传送中未受损。

3.2.4 结构化保护级

结构化保护级的可信计算基建立于一个明确定义的形式化安全策略模型之上,它要求将第3级系统中的自主和强制访问控制扩展到所有主体和客体。此外,还要考虑隐蔽通道。本级的可信计算基必须结构化为关键保护元素和非关键保护元素。可信计算基的接口也必须明确定义,使其设计与实现能经受更充分的测试和更完整的复审。本级加强了鉴别机制;支持系统管理员和操作员的职能;提供可信设施管理;增强了配置管理控制。系统具有相当的抗渗透能力。增加的内容主要表现在以下几方面。

(1) 可信计算基对外部主体能够直接或间接访问的所有资源(如主体、存储客体和输入输出资源)实施强制访问控制。

(2) 可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

(3) 系统开发者应彻底搜索隐蔽存储信道,并根据实际测量或工程估算确定每个被标识信道的最大带宽。

(4) 对用户的初始登录和鉴别,可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

3.2.5 访问验证保护级

访问验证保护级的可信计算基满足引用监视器需求,引用监视器仲裁主体对客体的全部访问。引用监视器本身是抗篡改的,必须足够小,能够分析和测试。为了满足引用监视器需求,可信计算基在其构造时,排除那些对实施安全策略来说并非必要的代码;在设计和实现时,从系统工程角度将其复杂性降低到最低程度。本级支持安全管理员职能;扩充审计机制,当发生与安全相关的事件时发出信号;提供系统恢复机制。系统具有很高的抗渗透能力。增加的内容主要表现在以下几方面。

(1) 在审计方面,可信计算基包含能够监控可审计安全事件发生与积累的机制,当超过阈值时,能够立即向安全管理员发出报警。并且,如果这些与安全相关的事件继续发生或积累,系统应以最小的代价中止事件发生。

(2) 可信路径上的通信只能由该用户或可信计算基激活,在逻辑上与其他路径上的通信相隔离,且能正确地加以区分。

(3) 可信计算基提供过程和机制,保证计算机信息系统失效或中断后,可以进行不损害任何安全保护性能的恢复。

3.3 安全操作系统的基本特征


视频讲解

3.3.1 最小特权原则

最小特权原则是系统安全中基本的原则之一。所谓最小特权指的是“在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权”。最小特权原则是指“应限定网络中每个主体所必需的最小特权,确保可能的事故、错误、网络部件的篡改等原因造成的损失最小”。

最小特权原则一方面给予主体“必不可少”的特权,这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作;另一方面,它只给予主体“必不可少”的特权,这就限制了每个主体所能进行的操作。

最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权,而角色允许主体以参与某特定工作所需要的最小特权进入系统。被授权拥有强力角色的主体,不需要动辄运用到其所有的特权,只有在那些特权有实际需求时,主体才去运用它们。如此一来,可减少由于不注意的错误或是侵入者假装合法主体所造成的损坏发生,限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用,从而使对特权无意的、没必要的或不适当的使用等情况不太可能发生。这种想法还可以引申到程序内部,只有程序中需要那些特权的最小部分才拥有特权。

3.3.2 访问控制

访问控制是主体依据某些控制策略或权限对自身或其资源进行不同授权的访问。访问控制的目的是限制访问主体对访问客体的访问权限,从而使计算机系统在合法范围内使用。访问控制又可以分为自主访问控制和强制访问控制。

访问控制三要素如下。

(1) 主体(Subject):可以对其他实体施加动作的主动实体,如用户、进程、I/O 设备等。

(2) 客体(Object):接受其他实体访问的被动实体,如文件、共享内存、管道等。

(3) 控制策略(Control Strategy):主体对客体的操作行为集和约束条件集,如访问矩阵、访问控制表等。

访问控制是操作系统安全机制的主要内容,也是操作系统安全的核心。访问控制的基本功能是允许授权用户按照权限对相关客体进行相应的操作,阻止非授权用户对相关客体进行任何操作,以此规范和控制系统内部主体对客体的访问操作。在系统中访问控制需要完成以下两种任务。

(1) 识别和确认访问系统的用户。

(2) 决定该用户可以对某一系统资源进行何种类型的访问。

1. 自主访问控制

自主访问控制(Discretionary Access Control,DAC)是一种最普遍的访问控制安全策略,其最早出现在 20 世纪 70 年代初期的分时系统中,基本思想伴随着访问矩阵被提出,在目前流行的操作系统(如 AIX、HP-UX、Solaris、Windows Server、Linux Server 等)中被广

泛使用,是由客体的属主对自己的客体进行管理的一种控制方式。这种控制方式是自由的,也就是说,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。在自主访问控制下,用户可以按自己的意愿,有选择地与其他用户共享他的文件。自主访问控制的实现方式通常包括目录式访问控制模式、访问控制表、访问控制矩阵和面向过程的访问控制等方式。

自主访问控制是基于对主体的识别限制对客体的访问,这种控制是自主的,在自主访问控制下,一个用户可以自主选择哪些用户能共享他的文件。其基本特征是用户所创建的文件的访问权限由用户自己控制,系统通过设置的自主访问控制策略为用户提供这种支持。也就是说,用户在创建了一个文件以后,其自身首先就具有了对该文件的一切访问操作权限,同时创建者还可以通过"授权"操作将这些访问操作权限有选择地授予其他用户,而且这种"授权"的权限也可以通过称为"权限转移"的操作授予其他用户,使具有使用"授权"操作的用户授予对该文件进行访问操作权限的能力。

2. 强制访问控制

强制访问控制(Mandatory Access Control,MAC)是"强加"给访问主体的,即系统强制主体服从访问控制政策。强制访问控制的主要特征是对所有主体及其所控制的客体(如进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。系统通过比较主体和客体的敏感标记决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其他客体的敏感标记,从而系统可以防止特洛伊木马的攻击。

强制访问控制一般与自主访问控制结合使用,并且实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制性访问限制检查后才能访问某个客体。用户可以利用自主访问控制防范其他用户对自己客体的攻击,由于用户不能直接改变强制访问控制属性,因此,强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户偶然或故意地滥用自主访问控制。

强制访问策略将每个用户及文件赋予一个访问级别,如最高秘密级(Top Secret,T)、秘密级(Secret,S)、机密级(Confidential,C)及无级别级(Unclassified,U)。其级别为 T>S>C>U,系统根据主体和客体的敏感标记决定访问模式。访问模式包括以下几个。

(1) 下读(Read Down):用户级别大于文件级别的读操作。

(2) 上写(Write Up):用户级别小于文件级别的写操作。

(3) 下写(Write Down):用户级别等于文件级别的写操作。

(4) 上读(Read Up):用户级别小于文件级别的读操作。

3.3.3 安全审计功能

安全审计是识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。其包括两方面的内容:一是采用网络监控与入侵防范系统,识别网络中的各种违规操作与攻击行为,即时响应(如报警)并进行阻断;二是对信息内容的审计,可以防止内部机密或敏感信息的非法泄露。

审计是安全系统的重要组成部分,在美国的 TCSEC 中对于安全审计的定义是这样的:一个安全系统中的安全审计系统是对系统中任一或所有安全相关事件进行记录、分析和再

现的处理系统。因此，在 TCSEC 中规定了对于安全审计系统的一般要求，主要包括以下 5 个方面。

(1) 记录与再现。要求安全审计系统必须能够记录系统中所有的安全相关事件，同时，如果有必要，应该能够再现产生系统某一状态的主要行为。

(2) 入侵检测。安全审计系统应该能够检查出大多数常见的系统入侵的行为，同时，经过适当的设计，应该能够阻止这些入侵行为。

(3) 记录入侵行为。安全审计系统应该记录所有的入侵行为，即使某次入侵已经成功，这也是事后调查取证和系统恢复必需的。

(4) 威慑作用。应该对系统中具有的安全审计系统及其性能进行适当宣传，这样可以对企图入侵者起到威慑作用，又可以减少合法用户在无意中违反系统的安全策略。

(5) 系统本身的安全性。安全审计系统本身的安全性必须保证，这包括两个方面的内容：一是操作系统和软件的安全性；二是审计数据的安全性。一般来说，要保证审计系统本身的安全，必须与系统中其他安全措施(如认证、授权、加密等)相配合。

另外，TCSEC 还要求 C2 级以上的安全操作系统必须包含审计功能。我国《计算机信息系统安全保护等级划分准则》对安全审计也有相应的要求。审计为系统进行事故原因的查询、定位、事故发生前的预测、报警及事故发生之后的实时处理提供详细、可靠的依据和支持，以便有违反系统安全规则的事件发生后能够有效地追查事件发生的地点和过程。

3.3.4 安全域隔离功能

安全域是指在其中实施认证、授权和访问控制的安全策略的计算环境。当安装和配置操作系统时，将创建称为管理域的初始安全域。安全域理论不仅为建设信息安全保障体系提供基础，而且在风险评估中如果能较好地应用安全域，还会起到事半功倍的作用。安全域可以将一个单独资产联系起来，在等级保护当中也有比较好的应用。总之，安全域理论是安全方面的最佳实践，对于信息安全建设具有非常重要的指导意义。

3.4 Windows 操作系统安全

视频讲解

从 1998 年开始，微软公司平均每年对自己的产品公布大约 70 份以上的安全报告，一直在坚持不懈地给人们发现的那些漏洞打补丁。Windows 这种操作系统之所以安全风险最高，主要是因为它的功能广泛和市场占有率高，从 NT 3.51 到 Windows 10，操作系统的代码差不多增加了几十倍，因为版本要更新，所以 Windows 系统上被悄悄激活的功能会越来越多，因此越来越多的漏洞会被人们发现。

3.4.1 远程攻击 Windows 系统的途径

(1) 对用户账户密码的猜测。登录 Windows 系统时主要的安全保护措施就是密码，通过字典密码猜测和认证欺骗的方法都可以实现对系统的攻击。

(2) 系统的网络服务。现代工具使存在漏洞的网络服务被攻击相当容易，点击之间即可实现。

(3) 软件客户端漏洞。诸如 IE 浏览器、MSN、Office 和其他客户端软件都受到攻击者

的密切监视,攻击者发现其中的漏洞,并伺机直接访问用户数据。

(4) 设备驱动。攻击者持续不断地分析操作系统上的无线网络接口,在USB和CD-ROM等设备提交的所有原始数据中发现新的攻击点。

例如,如果系统开放了服务器信息块(Server Message Block,SMB)服务,入侵系统最有效、最简单的方法是远程共享加载。试着连接一个发现的共享卷(如C$共享卷或IPC$),尝试各种用户名/密码组合,直到找出一个能进入目标系统的组合为止。其中,很容易用脚本语言实现对密码的猜测,如在Windows的命令行中用net use命令和for语句编写一个简单的循环就可以进行自动化密码猜测。

(5) 针对密码猜测活动的防范措施。使用网络防火墙限制对可能存在漏洞的服务(如在TCP 139和445号端口上的SMB服务、TCP 1355号端口上的MSRPC服务、TCP 3389号端口上的TS服务)的访问;使用Windows的主机防火墙(Windows XP和更高版本)限制对有关服务的访问;禁用不必要的服务(尤其注意TCP 139和445号端口上的SMB服务);制定和实施强口令字策略;设置一个账户锁定值,并确保该值已应用于内建的Administrator账户;记录账户登录失败事件,并定期查看事件日志文件。

3.4.2 取得合法身份后的攻击手段

1. 权限提升

在Windows系统上获得用户账户,之后就要获得Administrator或System账户。Windows系统最伟大的黑客技术之一就是所谓的GetAdmin系列,它是一个针对Windows NT4的重要权限提升攻击工具,尽管相关漏洞的补丁已经发布,该攻击所采用的基本技术"DLL注入"仍然具有生命力。因为GetAdmin必须在目标系统本地以交换方式运行,所以其强大的功能受到了限制。

对于权限提升的防范措施,首先要及时更新补丁,并且对于存储私人信息的计算机交互登录权限做出非常严格限制,因为一旦获得了这个重要的立足点之后,这些权限提升攻击手段就非常容易实现了。在Windows 2000和更高版本上检查交互登录权限的方法是运行"本地安全策略"工具,找到"本地策略"下的"用户权限分配"节点,然后检查"允许本地登录"权限的授予情况,如图3.2所示。

2. 获取并破解密码

获得相当于Administrator的地位之后,攻击者需要安装一些攻击工具才能更进一步地控制用户计算机,所以攻击者攻击系统之后的活动之一就是收集更多的用户名和密码。针对Windows XP SP2及以后的版本,攻击者侵入用户计算机后首先做的一件事就是关闭防火墙,因为默认配置的系统防火墙能够阻挡很多依赖于Windows网络辅助的工具制造的入侵。

对于密码破解攻击的防范措施,最简单的方法就是选择高强度密码,现在多数Windows系统都默认使用的安全规则——密码必须满足复杂性要求,创建和更改用户密码时要满足以下要求。

(1) 不能包含用户名和用户名字中两个以上的连贯字符。

(2) 密码长度至少要6位。

(3) 必须包含以下4组符号中的3组以上:大写字母(A~Z)、小写字母(a~z)、数字(0~9)、其他字符(如$、%、&、*)。

图 3.2　检查“允许本地登录”权限的授予情况

3.4.3　Windows 安全功能

1. Windows 防火墙

Windows XP 中有一个名为因特网连接防火墙(Internet Connection Firewall,ICF)的组件,微软公司在 XP 后续版本中对这个防火墙做了很多改进并把它重新命名为 Windows Firewall。改进的防火墙提供了更好的用户操作界面：保留了 Exception(例外)设置项,可以只允许“例外”的应用程序通过防火墙；新增加了一个 Advanced(高级)选项卡,用户可以对防火墙的各种细节配置做出调整。另外,现在还可以通过组策略配置防火墙,为需要对很多系统的防火墙进行分布式管理的系统管理员提供了便捷。

2. Windows 安全中心

Windows 安全中心可以让用户查看和配置很多系统安全防护功能：防火墙、自动更新、Internet 选项。Windows 安全中心的目标用户是普通消费者而并不是 IT 专业人员,这一点可以从它没有提供“安全策略”和“证书管理器”等高级安全功能配置界面上看出来。

3. Windows 组策略

怎样管理一个很大的计算机群组？这就需要组策略,它是功能非常强大的工具之一。所谓组策略,顾名思义,就是基于组的策略。它以 Windows 中的一个微软管理控制台(Microsoft Management Console,MMC)管理单元的形式存在,可以帮助系统管理员针对整个计算机或是特定用户设置多种配置,包括桌面配置和安全配置。例如,可以为特定用户或用户组定制可用的程序、桌面上的内容,以及“开始”菜单选项等,也可以在整个计算机范围内创建特殊的桌面配置。简而言之,组策略是 Windows 中的一套系统更改和配置管理工具的集合。组策略是修改注册表中的配置。当然,组策略使用自己更完善的管理组织方法,可

以对各种对象中的设置进行管理和配置,远比手工修改注册表方便、灵活,功能也更加强大。

组策略编辑器的启动很简单,只需执行“开始”→“运行”命令,在“运行”对话框中输入gpedit.msc,然后单击“确定”按钮即可启动Windows组策略编辑器。

例如,要启动Windows的文件保护功能,只需打开“组策略”窗口,在左侧列表中展开“计算机配置”→“管理模板”→“系统”→“Windows文件保护”节点,在右侧列表中显示已有的文件保护策略,如图3.3所示,双击列表中的某项,打开设置窗口。在该窗口中可设置“已启用”这一项安全策略。这样就实现了Windows的文件保护功能。

图3.3 Windows文件保护

4. 本地安全策略

Windows系统自带的“本地安全策略”是一个很不错的系统安全管理工具,它可以对本机的许多属性(如用户、密码、审核、用户权限分配等)进行设置,这些设置只影响本计算机的安全设置。

启用Windows的管理工具“本地安全策略”,依次执行“开始”→“程序”→“管理工具”→“本地安全策略”命令,打开“本地安全设置”窗口,如图3.4所示,主要包括账户策略、本地策略、公钥策略、IP安全策略配置。

5. Windows资源保护

从Windows 2000和Windows XP开始新增一项Windows文件保护(Windows File Protection,WFP)的功能,它能保护由Windows安装程序安装的系统文件不被覆盖。并且之后在Windows Vista版本中做了更新,增加了重要的注册键值和文件,并更名为Windows资源保护(Windows Resource Protection,WRP)。WRP有一个弱点,在于管理员用于更改被保护资源的访问控制列表(Access Control List,ACL)。默认设置下,本地管理

图 3.4　本地安全策略

员组使用 SeTakeOwnership 权限并接管任何受 WRP 保护资源的所有权。因此，被保护资源的访问权限可能被拥有者任意更改，这些文件也可能被修改、替换或删除。WRP 并非被用于抵御假的系统管理员，它的主要目的是防止第三方安装者修改对系统稳定性有重大影响的受保护文件。

6. 内存保护：DEP

微软公司的数据执行保护(Data Execution Prevention，DEP)机制由硬件和软件协同构成。DEP 机制将在满足其运行要求的硬件上自动运行，它会把内存中的特定区域标注为“不可执行区”——除非这个区域明确地包含着可执行代码。很明显，这种做法可以防止绝大多数堆栈型缓冲区溢出攻击。除了依靠硬件实现 DEP 机制外，Windows XP SP2 和更高版本还实现了基于软件的 DEP 机制以阻断各种利用 Windows 异常处理机制中的漏洞的攻击手段。Windows 体系的结构化异常处理(Structured Exception Handling，SEH)机制一直是攻击者认为最方便的可执行代码注入点。

3.4.4　Windows 认证机制

用户在使用 Windows 时总是要先进行登录。Windows 的登录认证机制和原理都是严格复杂的，理解并掌握 Windows 的登录认证机制和原理对用户来说很重要，能增强对系统安全的认识，并能够有效预防、解决黑客和病毒的入侵。

常见的 Windows 登录类型如下。

1. 交互式登录

交互式登录是最常见的登录类型，就是用户通过相应的用户账号和密码在本机进行登录。有人认为“交互式登录”就是“本地登录”，其实这是错误的。“交互式登录”还包括“域账号登录”，而“本地登录”仅限于“本地账号登录”。这里有必要提及的是，通过终端服务和远程桌面登录主机可以看作“交互式登录”，其验证的原理是一样的。

在交互式登录时，系统会首先检验登录的用户账号类型，是本地用户账号还是域用户账号，再采用相应的认证机制，因为不同的用户账号类型其处理方法也不同。

采用本地用户账号登录，系统会通过存储在本机安全账号管理器(Security Accounts Manager，SAM)数据库中的信息进行验证。这也就是为什么 Windows 2000 忘记 Administrator

密码时可以使用删除 SAM 文件的方法来解决。不过对于 Windows XP 以后的版本则不可以,可能是出于安全方面的考虑。用本地用户账号登录后,只能访问具有访问权限的本地资源。

采用域用户账号登录,系统则通过存储在域控制器的活动目录中的数据进行验证。如果该用户账号有效,则登录后可以访问到整个域中具有访问权限的资源。如果计算机加入域以后,登录对话框就会显示"登录到:"选项,可以从中选择登录到域还是登录到本机。

2. 网络登录

如果计算机加入工作组或域,当要访问其他计算机的资源时就需要"网络登录"了。当要登录主机时,输入该主机的用户名和密码后进行验证。这里需要提醒的是,输入的用户账号必须是对方主机上的,而非自己主机上的用户账号。因为进行网络登录时,用户账号的有效性是由对方主机验证的。

3. 服务登录

服务登录是一种特殊的登录方式。平时,系统启动服务和程序时,都是先以某些用户账号进行登录后运行的,这些用户账号可以是域用户账号、本地用户账号或 SYSTEM 账号。采用不同的用户账号登录,其对系统的访问、控制权限也不同,而且用本地用户账号登录只能访问具有访问权限的本地资源,不能访问到其他计算机上的资源,这点和"交互式登录"类似。

从任务管理器中可以看到,系统的进程所使用的账号是不同的。当系统启动时,一些基于 Win32 的服务会被预先登录到系统上,从而实现对系统的访问和控制。运行 services.msc 可以设置这些服务。正是因为系统服务有着举足轻重的地位,它们一般都以 SYSTEM 账号登录,对系统有绝对的控制权限,所以很多病毒和木马也争着加入这个账号。除了 SYSTEM 账号外,有些服务还以 Local Service 和 Network Service 这两个账号登录。而在系统初始化后,用户运行的一切程序都是以用户本身账号登录的。

从上面讲到的原理不难看出,平时使用计算机时要以 Users 组的用户登录,因为即使运行了病毒、木马程序,由于受到登录用户账号相应的权限限制,最多也只能破坏属于用户本身的资源,而对维护系统安全和稳定性的重要信息无破坏性。

4. 批处理登录

批处理登录一般用户很少用到,通常由执行批处理操作的程序使用。在执行批处理登录时,所用账号要具有批处理工作的权利,否则不能进行登录。

为了安全起见,平时进入 Windows 时都要输入账号和密码。而一般都是使用一个固定的账号登录的。面对每次烦琐的输入密码,有的人干脆设置为空密码或类似 123 等弱口令,而这些账号也多数为管理员账号。殊不知黑客用一般的扫描工具,很容易就能扫描到一段 IP 中所有弱口令的计算机,所以还是建议要把密码尽量设置得复杂些。

另外,账号和密码是明文保存在注册表中的,所以只要具有访问注册表权限的人都可以通过网络查看。因此,如果要设置登录,最好不要设置为管理员账号,可以设置为 Users 组的用户账号。

3.4.5 Windows 文件系统安全

文件系统安全是操作系统安全的核心。Windows 文件系统控制谁能访问信息以及能做些什么。即使外层账号安全被突破,攻击者也还必须击败文件系统根据文件拥有权和权

限精心设置的防御措施。当建立文件的权限时，必须先确定文件系统格式为 Windows 新技术文件系统（New Technology File System，NTFS），当然也可以使用文件配置表（File Allocation Table，FAT）格式，但是并不支持文件级的权限。一旦使用了 NTFS 的文件系统格式，就可通过 Windows 的资源管理器直接管理文件的安全。

NTFS 权限及使用有以下几个原则。

（1）权限最大原则。当一个用户同时属于多个组，而这些组又有可能被赋予了对某种资源的不同访问权限，则用户对该资源最终有效权限是在这些组中最宽松的权限，即加权权限，将所有的权限加在一起即为该用户的权限（“完全控制”权限为所有权限的总和）。

（2）文件权限超越文件夹权限原则。当用户或组对某个文件夹及该文件夹下的文件有不同的访问权限时，用户对文件的最终权限是访问该文件的权限，即文件权限超越文件的上级文件夹的权限，用户访问该文件夹下的文件不受文件夹权限的限制，只受被赋予的文件权限的限制。

（3）拒绝权限超越其他权限原则。当用户对某个资源有拒绝权限时，该权限覆盖其他任何权限，即在访问该资源的时候只有拒绝权限是有效的。当有拒绝权限时权限最大法则无效，因此对于拒绝权限的授予应该慎重考虑。

在同一个 NTFS 分区内或不同的 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。这时 NTFS 权限的继承性就起到了作用，关于 NTFS 权限的继承性有以下几方面。

（1）在同一个 NTFS 分区内移动文件或文件夹。在同一分区内移动的实质就是在目的位置将原位置上的文件或文件夹“搬”过来，因此文件和文件夹仍然保留有在原位置的一切 NTFS 权限（准确地讲，就是该文件或文件夹的权限不变）。

（2）在不同 NTFS 分区之间移动文件或文件夹。在这种情况下文件和文件夹会继承目的分区中文件夹的权限（ACL），实质就是在原位置删除该文件或文件夹，并且在目的位置新建该文件或文件夹（要从 NTFS 分区中移动文件或文件夹，操作者必须具有相应的权限。在原位置上必须有“修改”的权限，在目的位置上必须有“写”权限）。

（3）在同一个 NTFS 分区内复制文件或文件夹。在这种情况下复制文件和文件夹将继承目的位置中文件夹的权限。

（4）在不同 NTFS 分区之间复制文件或文件夹。在这种情况下复制文件和文件夹将继承目的位置中文件夹的权限（从 NTFS 分区向 FAT 分区中复制或移动文件和文件夹时都将导致文件和文件夹的权限丢失，因为 FAT 分区不支持 NTFS 权限）。

3.4.6 Windows 加密机制

加密文件系统（Encrypting File System，EFS）是 Windows 2003/XP 以上版本所特有的一个实用功能，NTFS 卷上的文件和数据都可以直接被操作系统加密保存，在很大程度上提高了数据的安全性。

EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的文件密钥（File Encryption Key，FEK），然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。随后系统利用公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加

密的文件时,系统首先利用当前用户的私钥解密FEK,然后利用FEK解密出文件。在首次使用EFS时,如果用户还没有公钥/私钥对(统称为密钥),则会首先生成密钥,然后加密数据。如果登录到了域环境中,密钥的生成依赖于域控制器,否则它就依赖于本地机器。

EFS加密有以下两点好处:首先,EFS加密机制和操作系统紧密结合,因此不必为了加密数据安装额外的软件,这节约了使用成本;其次,EFS加密系统对用户是透明的。也就是说,如果加密了一些数据,那么对这些数据的访问将是完全允许的,并不会受到任何限制。而其他非授权用户试图访问加密过的数据时,就会收到"访问拒绝"的错误提示。EFS加密的用户验证过程是在登录Windows时进行的,只要登录到Windows就可以打开任何一个被授权的加密文件。

要使用EFS加密,首先要保证操作系统符合要求。目前支持EFS加密的Windows操作系统主要有Windows 2000/XP及更新版本的操作系统。其次,EFS加密只对NTFS5分区上的数据有效(注意,这里提到的NTFS5分区是指由Windows 2003/XP格式化过的NTFS分区;而由Windows NT格式化的NTFS分区是NTFS4格式的,虽然同样是NTFS文件系统,但它不支持EFS加密),无法加密保存在FAT和FAT32分区上的数据。

对于想加密的文件或文件夹,只需要右击该文件或文件夹,从弹出的快捷菜单中选择"属性"命令,在打开对话框中的"常规"选项卡中单击"高级"按钮,在弹出的"高级属性"对话框中选中"加密内容以便保护数据"复选框,然后单击"确定"按钮,等待片刻,数据就加密好了。如果加密的是一个文件夹,系统还会询问是把这个加密属性应用到文件夹上,还是应用到文件夹及内部的所有子文件夹上,按照实际情况操作即可。解密数据也是很简单的,同样是按照上面的方法,取消对"加密内容以便保护数据"复选框的勾选,然后单击"确定"按钮。

注意:如果把未加密的文件复制到具有加密属性的文件夹中,这些文件将会被自动加密。若是将加密数据移出来,如果移动到NTFS分区上,数据依旧保持加密属性;如果移动到FAT分区上,这些数据会被自动解密。被EFS加密过的数据不能在Windows中直接共享。如果通过网络传输经EFS加密过的数据,这些数据在网络上将会以明文的形式传输。NTFS分区上保存的数据还可以被压缩,不过一个文件不能同时被压缩和加密。最后,Windows的系统文件和系统文件夹无法被加密。

3.4.7 Windows备份与还原

如果系统的硬件或存储媒体发生故障,"备份"工具可以保护数据免受意外的损失。例如,可以使用"备份"创建硬盘中数据的副本,然后将数据存储到其他存储设备。备份存储媒体既可以是逻辑驱动器(如硬盘)、独立的存储设备(如可移动磁盘),也可以是由自动转换器组织和控制的整个磁盘库或磁带库。如果硬盘上的原始数据被意外删除或覆盖,或因为硬盘故障而不能访问该数据,那么用户可以十分方便地从存档副本中还原该数据。为了保护服务器,应该安排对所有数据进行定期备份。数据备份的类型大致分为以下几种。

(1) 副本备份。可以复制所有选定的文件,但不将这些文件标记为已经备份(换言之,不清除存档属性)。如果要在正常备份和增量备份之间备份文件,复制是很有用的,因为它不影响其他备份操作。

(2) 每日备份。用于复制执行每日备份的当天修改过的所有选定文件。备份的文件将不会标记为已经备份(换言之,不清除存档属性)。

(3) 差异备份。用于复制自上次正常备份或增量备份以来所创建或更改的文件。它不将文件标记为已经备份(换言之,不清除存档属性)。如果要执行正常备份和差异备份的组合,则还原文件和文件夹将需要上次已执行过正常备份和差异备份。

(4) 增量备份。仅备份自上次正常备份或增量备份以来创建或更改的文件。它将文件标记为已经备份(换言之,清除存档属性)。如果将正常备份和增量备份结合使用,需要具有上次的正常备份集和所有增量备份集才能还原数据。

(5) 正常备份。用于复制所有选定的文件,并且在备份后标记每个文件为已经备份(换言之,清除存档属性)。使用正常备份,只需备份文件或磁带的最新副本就可以还原所有文件。通常,在首次创建备份集时执行一次正常备份。

组合使用正常备份和增量备份来备份数据,需要的存储空间最少,并且是最快的备份方法。然而,恢复文件可能比较耗时,而且比较困难,因为备份集可能存储在不同的磁盘或磁带上。

组合使用正常备份和差异备份来备份数据更加耗时,尤其当数据经常更改时,但是它更容易还原数据,因为备份集通常只存储在少量磁盘和磁带上。

Windows 自带的备份和还原工具如图 3.5 所示。

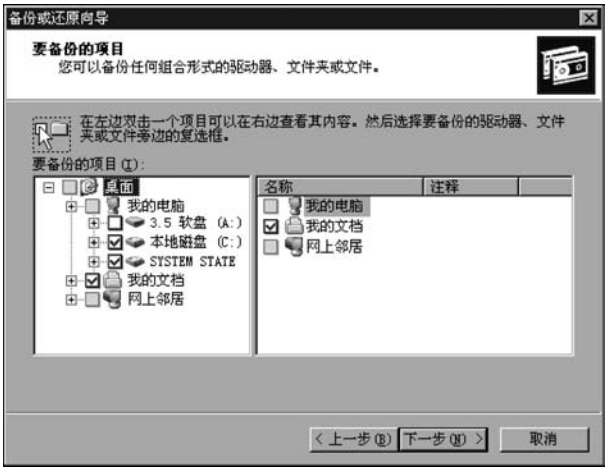

图 3.5　备份和还原工具

3.5　Android 操作系统安全

视频讲解

Android 是一个开放的移动设备操作系统。根据 IDC 2020 年的数据统计,Android 手机的市场份额为 84.1%。丰富的 Android 应用程序(简称应用)极大地方便了人们的生活,同时系统的安全性也越来越引起用户的关注。Android 应用可以操作设备上的各种硬件、软件,以及本地数据和服务器数据,并能够访问网络。因此,Android 操作系统为了保护数据、程序、设备、网络等资源,必须为程序提供一个安全的运行环境。

3.5.1　Android 安全体系结构

操作系统的安全性目的就是保护移动设备软件、硬件资源,包括 CPU、内存、外部设备、文件系统和网络等。Android 系统为了安全性,提供如下主要安全特征:操作系统严格的

图 3.6 Android 操作系统分层的安全体系结构

分层结构、应用沙盒、安全进程通信、授权和签名等。Android 作为开放平台,它的设计和实现细节完全暴露,因此对安全性要求更加严格,设计时首先要重点考虑的就是平台结构设计问题,Android 操作系统的安全体系结构设计为多层结构,如图 3.6 所示。这种结构在给用户提供安全保护的同时还保持了开放平台的灵活性。

Android 系统结构由 4 层组成,从上到下分别是应用层、应用框架层、系统运行类库层和 Linux 内核层。应用层由运行在 Android 设备上的所有应用构成,包括预装的系统应用和用户自己安装的第三方应用。大部分应用是由 Java 语言编写并运行在 Dalvik 虚拟机中;另一部分应用是通过 C/C++语言编写的本地应用。不论采用何种编程语言,两类应用运行的安全环境相同,都在应用沙箱中运行。应用框架层集中体现 Android 系统的组件设计思想。框架层由多个系统服务组成。Android 应用由若干个组件构成,组件和组件之间的通信是通过框架层提供的服务集中调度和传递消息实现的,而不是组件之间直接进行的。框架层协调应用层的应用工作,提升了系统的整体安全性。类库层主要由类库和 Android 运行时两部分组成。其中类库由一系列的二进制动态库构成,大部分来源于优秀的第三方类库,另一部分是系统原生类库,通常使用 C/C++语言开发。Android 运行时由 Java 核心类库和 Android 虚拟机 Dalvik 共同构成。Java 核心类库包括框架层和应用层所用到的基本 Java 库。Dalvik 是为 Android 量身打造的 Java 虚拟机,它与标准 Java 虚拟机(Java Virtual Machine,JVM)的主要差别在于 Dalvik 是基于寄存器设计的,而 JVM 是基于数据栈的,前者能够更快地编译较大的应用程序。Dalvik 允许在有限的内存中同时运行多个虚拟机的实例,每个 Dalvik 应用作为一个独立的 Linux 进程执行,可防止在某一虚拟机崩溃时所有应用都被关闭。最后一层是 Linux 内核层,该层提供的核心系统服务包括安全、内存、进程、网络和设备驱动等功能。

3.5.2 Linux 安全性

Android 平台的基础是 Linux 内核。Linux 操作系统经过多年的发展,已经成为一个稳定的、安全的、被许多公司和安全专家信任的安全平台。作为移动平台的基础,Linux 内核为 Android 提供了如下安全功能:基于用户授权的模式、进程隔离、可扩展的安全进程间通信(Inter-Process Communication,IPC)和移除不必要的不安全的内核代码。作为多用户操作系统,Linux 内核提供了相互隔离用户资源的功能。通过隔离功能,一个用户不能使用另一个用户的文件、内存、CPU 和设备等。

3.5.3 文件系统许可/加密

在 Linux 环境中,文件系统许可(Permission)可以保证一个用户不能修改或读取另一个用户的文件。Android 系统中每个应用都分配一个用户 ID,应用作为一个用户存在,因此,除非开发者明确指定某文件可以供其他应用访问,否则一个应用创建的文件其他应用不能读取或修改。文件系统加密功能可以对整个文件系统进行加密。内核利用 dm-crypt 技术创建加密文件系统。dm-crypt 技术是建立在 Linux 内核 2.6 版本的 device-mapper 特性之上的。device-mapper 是在实际的块设备之上添加虚拟层,以方便开发人员实现镜像、快

照、级联和加密等处理。为了防止系统口令攻击，如通过彩虹表（彩虹表就是将各种可能的数字、字母组合的哈希值预先计算好，通过查表的方式快速匹配，提高破解速度）或暴力破解等方法，口令采用 SHA1 加密算法进行保存。为了防止口令字典攻击，系统提供口令复杂性规则，规则由设备管理员制定，由操作系统实施。

3.5.4 Android 应用安全

Android 系统为移动设备提供了一个开源的平台和应用程序开发环境。通常程序开发语言采用 Java，并运行在 Dalvik 虚拟机中，对于游戏等性能要求较高的程序也可以采用 C/C++语言编写。程序安装包以. apk 为扩展名。一个应用程序通常由配置文件（AndroidManifest. xml）、活动（Activity）、服务（Service）、广播接收器（Broadcast Receiver）等组成。

1. Android 权限模式

所有的应用程序都运行在应用沙盒中，默认情况下，应用只能存取受限的系统资源。这种受限机制的实现方式有多种，包括不提供获取敏感功能的应用程序接口（Application Programming Interface，API）函数、采用角色分离技术和采用权限模式。权限模式最常用，通过这种方式把用于存取敏感资源的 API 函数只授权给值得信任的应用程序，这些函数主要涉及的功能包括摄像头、全球定位系统（Global Positioning System，GPS）、蓝牙、电话、短信、网络等。应用程序为了能够存取这些敏感资源，必须在它的配置文件中声明存取所需资源的能力。当用户安装这种程序时，系统会显示对话框提示程序需要的权限并询问用户是否需要继续安装。如果用户继续安装，系统就把这些权限授予对应的程序。安装过程中，针对用户只想授权其中的某些权限的情况系统是不支持的。安装完毕后，用户可以通过“系统设置”功能允许或拒绝某些权限。对于系统自带的应用程序，系统不会提示请求用户授权。如果程序的配置文件中没有指定受保护资源的授权，但程序中调用了资源对应的 API 函数，则系统抛出安全异常。程序的配置文件中还可以定义安全级别（Protection Level）属性，这个属性告诉系统其他哪些应用可以访问此应用。

2. 安全进程通信

尽管 Linux 内核提供了 IPC 机制，包括管道、信号、报文、信号量、共享内存和套接字等，但出于安全性考虑，Android 增加了新的安全 IPC 机制，主要包括 Binder、Service、Intent 和 ContentProvider。Binder 是一个轻量级的远程过程调用机制，它可以高效安全地实现进程内和进程间调用。Service 运行在后台并通过 Binder 向外提供接口服务，通常设有可见的用户界面。Intent 是一个简单的消息对象，此对象表示想要做某事的“意向”。ContentProvider 是一个数据仓库，通过它可以向外提供数据。例如，一个应用可以获取另一个应用通过 ContentProvider 向外公布的数据。在编写程序时如果需要进程通信，虽然可以使用 Linux 提供的传统方式，但还是推荐使用 Android 提供的安全 IPC 框架，这样可以避免传统方式存在的通信安全缺陷。

3. 应用程序安装包签名

所有的 Android 应用程序安装包（APK 文件）必须进行签名，否则程序不能安装在 Android 设备或模拟器中。签名的目的用于标识程序作者、升级应用程序。当没有签名的应用在安装时，包管理器就会拒绝安装。签名的应用在安装时，包管理器首先验证 APK 文件中的签名证书是否正确，如果正确，首先把应用放置在应用沙盒中，然后系统为它分配一

个UID,不同的应用有不同的UID;如果证书签名与设备中其他签名的应用相同,表示是同一个应用,则提示用户是否用新的应用更新旧的应用。该签名证书可以由开发者自己设定称之为自签名(Self-signed)证书,也可以由第三方的认证机构授权。系统提供自签名证书功能使开发者不再需要借助外部的帮助或授权即可以自己进行签名。Google公司提供了完整方便的签名工具为用户开发提供便利。

课后习题

一、选择题

1. Windows主机推荐使用(　　)格式。

A. NTFS　　B. FAT32　　C. FAT　　D. Linux

2. 下列对文件和对象的审核,错误的一项是(　　)。

A. 文件和对象访问的成功和失败　　B. 用户及组管理的成功和失败

C. 安全规则更改的成功和失败　　D. 文件名更改的成功和失败

3. 下列不属于服务器的安全措施的是(　　)。

A. 保证注册账户的时效性　　B. 删除死账户

C. 强制用户使用不易被破解的密码　　D. 所有用户使用一次性密码

4. 下列不属于数据备份类型的是(　　)。

A. 每日备份　　B. 差异备份　　C. 增量备份　　D. 随机备份

5. TCSEC是(　　)国家标准。

A. 英国　　B. 意大利　　C. 美国　　D. 俄罗斯

6. 身份认证的含义是(　　)一个用户。

A. 注册　　B. 标识　　C. 验证　　D. 授权

7. 口令机制通常用于(　　)。

A. 认证　　B. 标识　　C. 注册　　D. 授权

8. 在生成系统账号时,系统管理员应该分配给合法用户一个(　　),用户在第1次登录时应更改口令。

A. 唯一的口令　　B. 登录的位置

C. 使用的说明　　D. 系统的规则

9. 信息安全评测标准CC是(　　)标准。

A. 美国　　B. 国际　　C. 英国　　D. 澳大利亚

10. (　　)数据备份策略不是常用类型。

A. 完全备份　　B. 增量备份　　C. 选择性备份　　D. 差异备份

11. 数据保密性安全服务的基础是(　　)。

A. 数据完整性机制　　B. 数字签名机制

C. 访问控制机制　　D. 加密机制

12. Windows系统的用户账号有两种基本类型,分别为全局账号和(　　)。

A. 本地账号　　B. 域账号　　C. 来宾账号　　D. 局部账号

13. Windows系统安装完成后,默认情况下系统将产生两个账号,分别为管理员账号

和(　　)。

A. 本地账号　　B. 域账号　　C. 来宾账号　　D. 局部账号

14. 某公司的工作时间是上午 8 点半至 12 点,下午 1 点至 5 点半,每次系统备份需要一个半小时,下列适合作为系统数据备份的时间是(　　)。

A. 上午 8 点　　B. 中午 12 点　　C. 下午 3 点　　D. 凌晨 1 点

15. 下列不是 UNIX/Linux 操作系统的密码设置原则的是(　　)。

A. 密码最好是英文字母、数字、标点符号、控制字符等的组合

B. 不要使用英文单词,容易遭到字典攻击

C. 不要使用自己、家人、宠物的名字

D. 一定要选择字符长度为 8 位的字符串作为密码

16. 1999 年,我国发布第 1 个信息安全等级保护的国家标准 GB 17859—1999,提出将信息系统的安全等级划分为(　　)个等级。

A. 7　　B. 8　　C. 4　　D. 5

17. 定期对系统和数据进行备份,在发生灾难时进行恢复。该机制是为了满足信息安全的(　　)属性。

A. 真实性　　B. 完整性　　C. 不可否认性　　D. 可用性

二、填空题

1. _____年,欧共体发布了《信息技术安全评价准则》。_____年,加拿大发布了《加拿大可信计算机产品评价准则》。

2. 计算机安全评价标准(TCSEC)是计算机系统安全评估的第 1 个正式标准,于_____年 12 月由美国国防部公布。

3. D1 系统只为_____和_____用户提供安全保护。

4. C 类安全等级可划分为_____和_____两类。

5. 计算机系统安全评估的第 1 个正式标准是_____。

6. 自主访问控制(DAC)是一个接入控制服务,它执行基于系统实体身份及系统资源的接入授权。这包括在文件、_____和_____中设置许可。

7. 安全审计是识别与防止_____、追查_____的重要措施之一。

8. C1 系统的可信任运算基础体制,通过将_____和_____分开达到安全的目的。

9. _____账号一般是在域中或计算机中没有固定账号的用户临时访问域或计算机时使用的。

10. _____账号被赋予在域中和在计算机中具有不受限制的权利,该账号被设计用于对本地计算机或域进行管理,可以从事创建其他用户账号、创建组、实施安全策略、管理打印机及分配用户对资源的访问权限等工作。

11. 中华人民共和国国家标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》已经正式颁布并使用。该准则将信息系统安全分为 5 个等级,分别是自主保护级、_____、_____、_____和访问验证保护级。

12. B2 级别的系统管理员必须使用一个_____、_____的安全策略模式作为系统的可信任运算基础体制。

13. B3 级别的系统具有很强的_____和_____。

14. 访问控制三要素为主体、_____和_____。

15. 自主访问控制的实现方式通常包括目录式访问控制模式、_____、_____和面向过程的访问控制等方式。

16. 组策略是 Windows 中的一套系统_____和_____管理工具的集合。

17. Android 系统结构由 4 层组成,从上到下分别是应用层、应用框架层、_____和_____。

三、简答题

1. 简述 TCSEC 中 C1、C2、B1 级的主要安全要求。

2. 简述审核策略、密码策略和账户策略的含义。这些策略如何保护操作系统不被入侵?如何关闭不需要的端口和服务?

3. 计算机安全评价标准中 B 类安全等级都包括哪些内容?

4. 计算机安全评价标准中 A 类安全等级都包括哪些内容?

5. 计算机信息系统安全保护等级划分准则中将信息系统安全分为几个等级?主要的安全考核指标是什么?

6. 安全操作系统的基本特征有哪些?

7. 安全审计主要包括哪几方面的内容?

8. 远程攻击 Windows 系统的途径有哪些?

9. 取得合法身份后的攻击手段有哪些?

10. Windows 安全功能有哪些?

11. 常见的 Windows 的登录类型有哪几种?

12. NTFS 权限及使用原则有哪些?

13. NTFS 权限的继承性有哪几方面的内容?

14. 文件加密系统的原理是什么?

15. 数据备份的类型大致分为哪几种?

16. 本地安全策略由哪几部分组成?