信息系统安全——董开坤

第一章 绪论

1.1 信息技术的告诉发展和网络空间安全态势

网络空间安全已扩展至诸多领域，呈现出*综合性*和*全球性*的新特点。

1.2 网络空间安全的基本概念

信息的安全属性：机密性、完整性、可用性、可控性、可鉴别性。

方院士提的网络空间安全概念。

网络空间安全的核心内涵仍是信息安全

1.3 网络空间面临的安全威胁

威胁的来源：环境因素、意外事故或故障；无恶意的内部人员；恶意的内部人员；第三方；外部人员攻击。

威胁的层次：设备层（物质基础）；系统层；数据层；应用层。

1.4 网络空间安全的技术体系

新技术体系：应用层；数据层；代码层；硬件层

1.5 信息系统安全技术

信息系统是信息的载体

安全认证：对实体身份进行审核，证实其合法性的过程

访问控制：限制信息系统中主体对客体的访问，使系统在授权范围内使用

安全审计：对信息系统中与安全相关的活动和进行记录、检查及审核

操作系统安全：使信息系统安全的基础

数据库安全：维护数据库系统的运行安全，保障数据库中的数据信息的安全

恶意代码及其防范：是对信息系统危害最大的攻击之一

信息系统安全测评：这一章讲了半节课。。。

可信计算：这是最后一章，都没讲吧

信息系统安全防护的基本原则：整体性原则；分层性原则；最小特权原则

第二章 安全认证

2.1 安全认证概述

定义：对实体身份进行审核，证实其合法性的过程

作用：识别合法实体与非法实体；信息系统的第一道安全防线，是其他安全机制的基础

认证基本过程：标识、鉴别

标识

定义：为每个实体取一个系统可以识别的内部名称

作用：追踪和控制实体在系统中的行为

特点：具有唯一性，通常是公开的

生成方式：用户提供、系统提供

载体：人工记忆、令牌、不需要载体

鉴别

定义：实体标识与实体联系的过程

作用：证实实体是否名副其实的有效

特点：鉴别过程应该是私密的

2.2 基于知识的身份认证

定义：根据用户掌握的知识对其进行身份认证

最普遍的技术：基于口令的身份认证

口令生成要求：字符的选择、长度、对管理员保密

口令保护：完整性、机密性

动态口令技术：又叫动态令牌、动态密码，一句用户身份信息，并引入不确定因子，产生随机变化的口令

技术实例——口令序列（S/KEY）：初始化>>生成口令序列>>口令的使用和验证

2.3 基于令牌的身份认证

令牌：持有人的身份标识，唯一、易识别、不易伪造

常见的令牌：智能卡、USB Key

2.4 基于生理特征的身份认证

优点：不易被仿冒、模仿；不需要载体；不易丢失和被偷窃

缺点：需要特殊硬件；不够稳定；有时不被接受；长期不变

2.5 基于行为特征的身份认证

笔迹、步态、击键动力学、发展情况

认证系统的误判情况：错误拒绝率（FRR）；错误接受率（FAR）

认证系统的准确性：交叉错判率（CER）

2.6 人工交互认证（无）

2.7 多因素和附加认证技术

组合两种或以上的认证技术，以提高安全性或可用性

第三章 访问控制

3.1 访问控制概述

客体定义：包含或接收信息的被动实体

主体定义：可导致信息在客体间流动，或使系统状态发生变化的主动实体

授权定义：规定主体可以对客体执行的动作

安全策略定义：一种将系统状态划分为安全态（授权态）和非安全态（未授权态）的声明。

引用监控器定义：对主体访问客体的行为进行仲裁的抽象装置

访问控制使保证信息系统安全最重要的核心策略之一

3.2 自主访问控制

自主访问控制策略（DAC）策略下，每个客体有且仅有一个属主；客体的属猪可以按照自己的意愿精确地指定主体对于客体地访问权限

严格的 DAC：客体的属主不允许其他用户代理客体的权限管理

自由的 DAC：可以的属主允许其他用户代理客体的权限管理，可以多次转让

属主可以转让的 DAC

实现方式

访问口令：每个客体至少有一个访问口令，通过口令实现对主体的访问，这个口令不同于身份认证的口令。

访问控制矩阵：用矩阵表示一个自主访问控制系统；

特点：最原始访问控制方法；直观，任何访问控制策略均可以被模型化为访问矩阵形式；开销大，不易扩展、管理

访问能力表：主体可访问的客体明细表，表中的每一项包含客体的标识，主体对客体的访问权限。

访问控制表：在每个客体上附加主体明细表，表中的每一项包含主体身份和主体对该客体的访问权限

特点：以客体为基准；灵活、易用、直观；应用最广泛的访问控制方法；Unix、Windows 都使用了该方法进行访问控制

授权关系表：对于访问控制表的每一个非空元素的实现方法，既不对应于行，也不对应于列

特点：授权关系表中的每一行表示了主体和客体的一个权限关系；如果这张表按主体进行排序，可以拥有访问能力表的优势；如果这张表按客体排序，可以拥有访问控制表的优势；特别适合关系数据库。

属主/同组用户/其他用户：在文件属性中附加一段有关控制信息的二进制位，分别对应三类用户访问权限，应用于 UNIX/Linux 系统中

特点：简易、易于实现、高效；于 ACL 相比，访问控制粒度较粗

自主访问控制的局限性：客体属主决定该客体的保护策略，存在安全缺陷；允许在主体间传递访问权限，过程中可能改变访问权限关系，存在安全隐患。

3.3 强制访问控制

客体的拥有者无权传播该客体的访问权限；主体不能改变自己、自己所拥有客体、其他主体、以及其他所有客体的安全属性

特点：系统对授权集中管理；管理部门严格按照规则设置系统中客体、主体的安全级别、安全范畴等安全属性；系统运行时通过比较主、客体的安全属性，决定是否允许主体以其所请求的方式访问客体

多级安全

保密规定 1：如果某人的安全级别达不到信息的安全级别，则禁止把该信息传播给他

保密规定 2：如果某人的安全级别达到了信息的安全级别，则允许把该信息传播给他

支配（Dominate，dom）——偏序关系：密级大于等于，范畴包含

BLP 模型（目标：机密性）

第一个经过严格数学证明的安全模型

主体对客体的访问权限：只读、添加、执行、读写

SS-策略：主体 S 可以对客体 O 进行读访问，仅当 S 的安全级别支配 O 时

*-策略：主体 S 可以对客体 O 进行写访问，仅当 O 的安全级别支配 S 时

DS-策略：主体 S 可以访问客体 O，仅当 S 具备对 O 的自主访问权限

特性：强制特性、自主特性

*-策略对系统可用性的影响：高级主体只能生产高级信息，有的系统可能无法正常运行

隐蔽通道：如果一个通信信道不是设计用于通信，也不是有意用于传递信息的，则称通信信道是隐蔽的；允许进程以违反系统安全策略的方式传递信息的通道

Biba 模型（目标：完整性）

数据完整性的四类（五种）定义：数据质量符合预期；防范对数据的不正确

修改，防范对数据的非授权修改；禁止修改数据，或可检测对数据的任何修改；限制信息单向流动

完整性定义：<C, S>，主、客体完整性等级的含义不完全相同（可信可靠，重要安全）

访问方式：读、写、调用

严格完整性策略（SIP）：不下读；不上写；支配调用

环策略（RP）：任意读；不上写；支配调用

针对主体的下限标记策略（LWMPS）：任意读后主体级别取主、客体最低级别；不上写；支配调用

针对客体的下限标记策略（LWMPO）：不下读；任意写后客体级别取最低；支配调用

下限标记完整性审计策略（LWMIAP）：不下读；任意写，当 S 不支配 O 时进行审计；支配调用

BLP 的机密性级别和 Biba 的完整性级别没有必然联系

3.4 基于角色的访问控制（RBAC）

传统访问控制在授权管理方面的局限性：授权工作量于用户数、客体数成正比；用户职责变化时重新授权工作量大；用户离职时的权限撤销工作量大

用户通过角色获得权限；必须支持多对多的用户-角色指派；必须支持多对多的权限-角色指派；必须支持用户-角色检查；用户可同时行驶多个角色的权限

职责分离（SOD）：角色的执行权限和管理权限时分离的，主体不应同时拥有二类权限；将不同责任分派给不同主体以期达到相互牵制，消除一个主体执行两项或多项不相容任务的风险

静态职责分离（SSD）：如果两个角色存在 SSD 约束，则当一个用户分配了其中一个角色时，就不能再获得另一个角色；不能在有 SSD 约束关系的两个角色之间定义继承关系

动态职责分离（DSD）：权限约束作用于用户会话激活角色的阶段；如果两个角色存在 DSD 约束，用户不能在一个会话中同时激活这两个角色

特点：中性，可以偏自主，也可以偏强制；灵活，可以适应变化的需求；支持职责分离原则；支持最小特权原则

3.5 最小特权管理

定义：不受访问控制策略的限制

特权存在原因：便于系统维护；提高系统可用性

危害：被窃取；被滥用；被误用

最小特权：主体只能被授予其完成任务所必需的特权

最小特权原则：限定每个主体所必须的最小特权，确保可能发生的事故、错误等原因造成的损失最少

最小特权原则的基本思想：**分权**，把超级用户权限进行细分，分别授予不同系统操作员或管理员，确保每一个用户都没有足够的权限去破坏整个系统

第四章 安全审计

4.1 安全审计概述

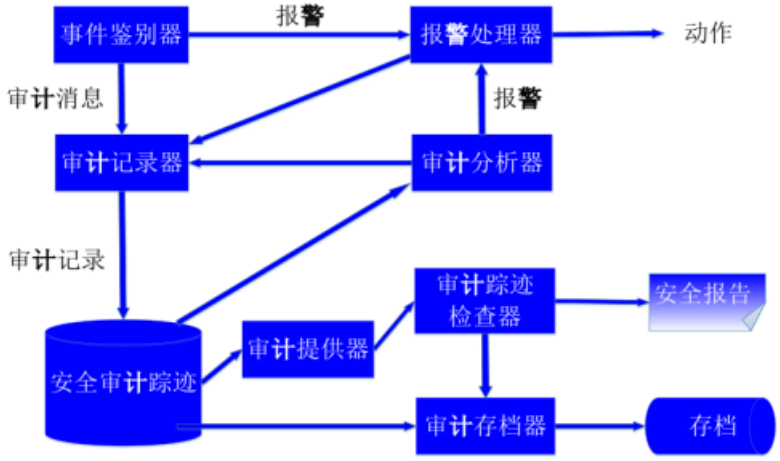
概念：对信息系统中于安全相关的活动进行记录、检查及审核的过程

目的：检测、阻止非授权用户对系统的入侵；检测、显示授权用户的误操作

安全目标：跟踪、监视信息系统中的异常事件（直接）；监视系统中其他安全机制的运行情况和可信度（间接）
审计事件：信息系统审计用户操作的最基本单位
审计踪迹：关于操作系统、应用程序或用户活动的一组记录
作用：系统安全的最后防线，访问控制的必要补充；重建事件，监测入侵，故障监测，发现系统不足，与其他安全机制联动
审计过程是一个独立的过程，应与系统其他功能相隔离；同时，要求系统必须能够生成、维护及保护审计过程，使其免遭修改、非法访问及毁坏，特别要保护审计数据，严格限制未经授权的访问

4.2 安全审计系统模型

数据生成：标识审计级别，列举可审计事件的类型；指定与动作相关的用户身份
事件选择：选择或排除一些事件；使系统可以配置不同级别的审计粒度
事件存储：创建并维护安全审计踪迹；提供可用性，防止审计踪迹数据丢失
自动响应：当存在安全违规时产生自动的响应
审计分析：提供自动化机制，分析系统活动和审计数据；标识可审计事件集合，确定是否已经发生违规
审计复合：对于授权用户，帮助对审计数据的审核
X.816 标准定义的审计系统模型



事件鉴别器对每个检测到的事件，以审计消息的形式传输到审计记录器
审计记录器为每个事件创建格式化的审计记录并将其存储到安全审计踪迹中
审计分析器基于活动模式，可以定义新的可审计事件，并发送到审计记录器中，也可以产生报警
报警处理器可以根据收到的报警信息采取一系列措施，这些报警信息通常是可审计事件
审计存档器是一个软件模块，定期从安全审计踪迹中提取记录，创建可审计事件的一个永久存档
审计提供器是一个与应用程序和安全审计踪迹相关的用户接口
审计踪迹检查器是一个应用程序或用户，可以检查审计踪迹和审计存档的历史数据，可以提供人工可读的安全报告
根据审计数据不同的应用层次，安全审计模型可划分为四个部分
　　审计数据创建层：负责审计数据的创建，包括任何可以产生审计数据的程序或模块，例如程序调试器、审计踪迹合成工具、系统监视器

审计记录管理层：审计数据的解析、转换和管理，例如记录、重放、接合、压缩、存储和获取等

审计记录缩减层：将底层审计数据归纳抽象为适合审计应用程序使用的较高层次的数据，并负责翻译、筛选审计踪迹、去除无用的数据，减少审计记录的数量并提高审计数据的有效性，例如实体关系分析、行为抽象

审计记录分析应用层：进行入侵检测、图形用户界面、审计信息浏览、网络和系统监视、安全分析等更高层次的推论和抽象

4.3 安全审计系统的设计与实现

确定审计策略

分析要审计的事件类型：注册事件、使用系统的事件、利用隐蔽通道的事件

确定审计的事件集：明确对哪些事件进行审计，并非所有事件都要审计

设置审计踪迹：审计踪迹维护系统活动的记录，通常可以分为系统级审计踪迹、应用级审计踪迹、用户级审计踪迹、物理访问审计踪迹

定义审计记录：时间、地点、主体、客体、操作、结果

确定审计点：确定在信息系统中哪些点可以捕获到所有需要的审计事件

审计记录的存储：存储形式（日志文件、数据库等形式）；存储位置（本地/异地）

审计记录的安全性要求：完整性要求，机密性要求，可用性要求

审计信息的使用与管理：审计记录的查阅，审计记录的分析，审计信息的管理，审计信息的维护

审计系统的构成：审计发生组件（捕获），日志记录组件（记录），日志分析组件（分析），事件报告组件（报告），审计管理组件（系统管理）

降低审计开销：有选择地审计，开辟审计缓冲区，设法节约磁盘空间

第五章 Windows 操作系统安全

5.1 操作系统安全基础

操作系统是信息系统资源的基本控制器——这使其成为主要的攻击目标

操作系统的安全目标：允许多用户安全的共享单机；确保网络环境下的安全操作；保护对象和保护方法

保护对象：内存；可共享的 I/O 设备；可连续复用的 I/O 设备；可共享的程序或子程序；网络；可共享数据

安全保护的基本原理：访问控制；隔离控制；认证；安全通信；安全审计；入侵检测；恢复

隔离控制包括物理隔离、时间隔离、逻辑隔离、加密隔离

保护方法：内存保护模式；CPU 运行模式；系统调用

内存保护：操作系统进程、用户进程具有不同的权限

CPU 运行模式——系统模式：可以执行任意指令、访问任意内存地址、硬件设备、中断操作、改变处理器特权状态、访问内存管理单元、修改寄存器

CPU 运行模式——用户模式：受限的内存访问，有些指令不能执行；不能停止中断，改变任意进程状态，访问内存管理单元等

CPU 运行模式——系统调用：从用户模式进入内核模式的系统程序，是用户程序和内核交互的接口；系统调用不能更改；可分为进程控制、文件管理、设备管理、信息维护、通信等类别

内核实现方法——单核：一个大内核提供所有服务，包括文件系统、网络服务、

设备驱动等；高效，但复杂，某部分的 bug 会影响整个系统
内核实现方法——微内核：内核较小，仅提供执行系统服务必须的机制；可实现最小特权，容忍设备驱动的失败/错误等，但性能差，系统的关键服务出错会使得系统停机
备份/恢复策略：整体备份（一个备份周期内的数据完全备份），增量备份（只备份上次备份以后有变化的数据），实时备份（持续跟踪目标数据的改变，并将其备份）
可信计算机系统评估准则 TCSEC 对计算机的安全级别进行了分类，由低到高分为 D、C、B、A 级

D 类安全等级只包括 D1 一个级别，安全等级最低，系统制位文件和用户提供安全保护；最普通的形式是本地操作系统或者一个完全没有保护的网络

C 类安全等级，自主保护类，能够提供审计和保护，为用户的行动和责任提供审计能力

C1 级：自主安全保护系统。系统的可信任运算基础体制（TCB），通过将用户和数据分开来达到安全的目的，C1 系统中用户认为系统中所有文档都具有相同的机密性

C2 级：受控存取控制系统。比 C1 系统加强了可调的审计控制，通过登录过程、安全事件和资源隔离来增强这种控制

B 类安全等级，强制保护类。具有强制性保护功能，用户若没有与安全等级相连，系统不允许其存取对象

B1 安全级：标记安全保护级；系统对每个对象设置灵敏度标记，使用灵敏度标记作为强制访问控制的基础；系统必须通过审计来记录未授权访问的企图

B2 安全级：结构保护级；满足 B1 要求基础上，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

B3 安全级：安全域级；符合 B2 所有安全需求，具有很强的监视委托管理访问能力和抗干扰能力，必须设有安全管理员

A 类安全级：验证保护级，级别最高，目前仅包含 A1 一个安全类别

A1 级：系统的设计者必须按照一个正式的设计规范来分析系统，设计者必须运用核对技术来确保系统符合设计规范

5.2 Windows 安全概述

C2 级安全功能：安全登录、自主访问控制、安全审计、客体重用
B 级安全功能——可信通路：主要应用在用户登录或注册时，保证用户确实是和安全核心通信，防止不可信进程模拟系统的登录过程而窃取口令
可信通路的实现：用户在执行敏感操作前，向安全内核发送“安全注意符”来触发和构建用户与安全内核间的可信通路，一般由安全注意键（系统指定的组合按键）来激活
Windows 操作系统采用用户模式和核心模式分离的体系结构；用户模式下的软件在五特权的状态下运行，系统资源访问权限有限；所有对核心模式的访问都是受保护的，避免失控的用户进程破坏处于核心模式下的低层次的系统驱动程序

活动目录

是 windows 分布式联网的基础，是一个包含网络资源的数据库，也是一种分布式的目录服务系统

域是 windows 网络系统的安全性边界；活动目录的安全管理单元是域，域中的所有用户和计算机执行相同的域安全策略；当用户使用域账户而非本地账户登

录时，Windows 客户端会使用活动目录来认证

Winlogon 进程

用户登录程序；系统启动自动启动的一个程序；负责管理用户登录和注册的过程，并监视安全认证的顺序

程序：System32\Winlogon.exe

功能：负责响应 SAS；管理交互式登录会话

图形化标识和验证

GINA，为用户提供图形化的交互式登录对话框，包括几个动态库文件，被 Winlogon 进程调用，GINA 调用 LSA

程序：System32\Msgina.dll，运行在 Winlogon 进程中

功能：获得用户的名称，获得用户口令或智能卡的 Pin 码

本地安全认证 LSA

安全子系统的核心组件，负责加载认证包，管理域间的信任关系，确认 SAM 中的数据，控制各种类型的用户进行本地和远程登录

程序：System32\lsass.exe，System32\lsasrv.dll（主要由该模块实现）；存在于用户模式的进程 lsass.exe 中，分则管理、执行 Windows 的本地安全策略，在账户登录到系统时发放安全令牌；将 SAM 产生的审计信息保存在日志文件中

Lsass 策略数据库位置——HKEY_LOCAL_MACHINE\SECURITY；内容——哪些域是可信任的；允许哪些用户以何种方式登录系统；授予用户哪些权限

Kerberos 身份认证

Windows 的域身份认证协议；使用 Windows 操作系统之间以支持 Kerberos 身份认证的客户之间的身份认证；运行在 Lsass 进程环境下的 DLL，实现 Kerberos 认证协议

MSV1.0 身份认证

为不支持 Kerberos 身份认证的 Windows 客户提供基于 NTLM 的身份认证；Msv1_0.dll，运行在 Lsass 进程环境下的 DLL，实现 LAN Manager 2 协议

NTLM 工作流程：用户通过输入 Windows 账号和密码登录客户端主机>>服务器收到请求后，生成一个 16 位的随机数>>客户端在接收到服务器发回的 Challenge 后，用第一步中保存的密码哈希值对其加密，然后再将加密后的 Challenge 发送给服务器>>服务器接收到客户端发送回来的加密后的 Challenge，会向 DC 发送针对客户端的验证请求>>DC 根据用户名获取该账号的密码哈希值，对原始的 Challenge 进行加密，与服务器发送的客户端加密的 Challenge 进行对比验证，将验证结果发回给服务器，并最终反馈给客户端

安全账户管理器 SAM

SAM 数据库存储本地用户和本地组的账户以及相关安全信息；当用户用本地战虎登录到计算机时，SAM 进程（samsrv）获得登录信息并查询 system32\config 目录下的 SAM 数据库，如果有匹配的认证，用户就可以登录系统；SAM 文件是二进制模式的，而不是文本格式的，口令用 MD4 散列算法存储

程序：System32\Samsrv.dll，运行于 Lsass 进程中

功能：提供一组管理本地用户和用户组的子进程

位置：HKEY_LOCAL_MACHINE\SAM

内容：本地用户和用户组、以及它们的口令、账户限制；系统的管理员恢复账号及口令

安全引用监视器 SRM

内核模式组件，执行对象访问合法性检查、产生审计日志条目、提供用户权限

Netlogon 进程

Winlogon 处理本地键盘登录，Netlogon 处理网络登录；维护计算机到其所在域内的域控制器的安全信道；域登录时用到的，建立安全信道，用户名、密码在信道里是加密传输的

程序：System32\Netlogon.dll

5.3 Windows 本地安全机制

本地用户账户：创建于网络客户机，作用范围限于创建它的计算机，用户控制用户对该计算机上资源的访问

全局用户账户：创建与服务器，可以在网络中任何计算机上登录，使用范围是整个网络

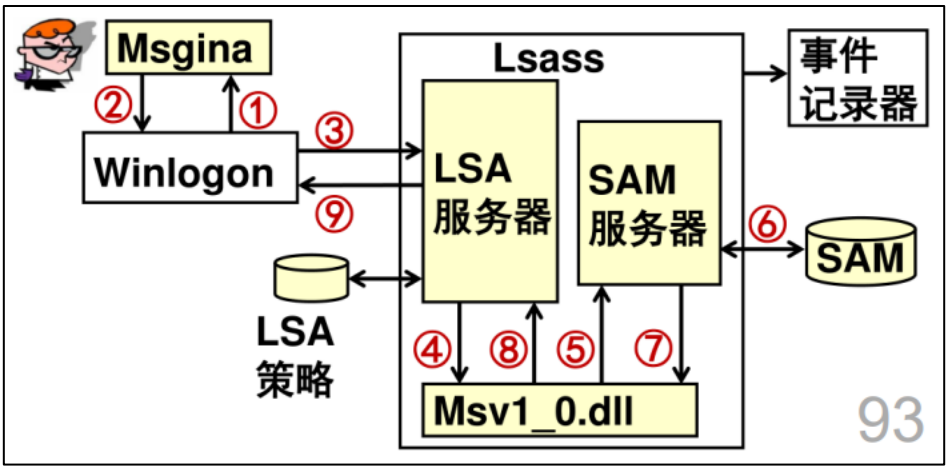
内置账户：Administrator（管理员账户，具有最高权限）；Guest（来宾账户）

普通用户：由系统管理员建立，通过用户的配置文件存储账户的唯一安全标识 SID 和权限

安全标识符（SID）：每次创建一个用户或一个组的时候，系统会给它分配一个唯一的 SID；用户名与 SID 一一对应，删除用户后 SID 不会被重用

SID 的唯一性，SID 永远都是唯一的，由计算机名、当前时间、当前用户态线程和 CPU 耗费时间的总和共同确定，永远不会更改

Windows 本地身份认证机制



用户按下 SAS 键后，立即引起硬件中断，并被操作系统捕获，操作系统将激活 Winlogon 进程

GINA 将用户输入的账号和口令返回给 Winlogon 进程

Winlogon 进程将用户名和口令信息发送给 LSA 进行验证

LSA 调用 Msv1_0.dll 验证程序包，将用户信息处理后生成密钥

Msv1_0.dll 验证程序包将生成的密钥发送给 SAM 服务器进程

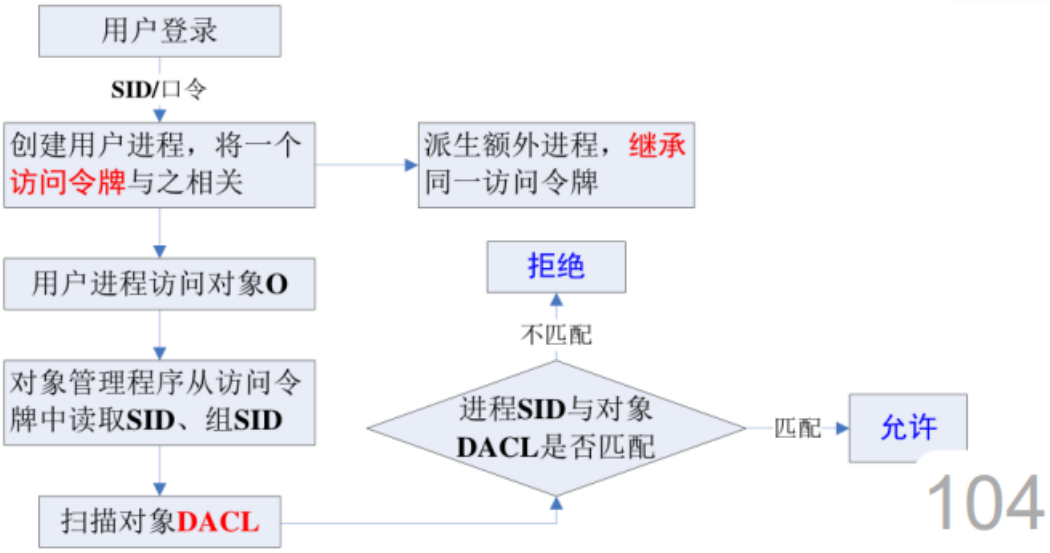
SAM 服务器进程将收到的用户密钥，与 SAM 数据库中存储的密钥对比

若用户身份合法，SAM 进程会将用户的 SID、用户组 SID 和相关信息发给 Msv1_0.dll 验证程序包

Msc1_0.dll 验证程序将认证结果信息返回给 LSA

LSA 根据收到的 SID 信息创建安全访问令牌，然后将令牌的句柄和登录信息发送给 Winlogon 进程

Windows 访问控制机制的工作流程



访问令牌：用户通过身份认证后，登录进程会为其创建一个访问令牌

用来标识进程或线程（主体）的安全属性：用户 SID 和组 SID，进程权限信息，信息字段，默认的自主访问控制列表（DACL）

安全描述符：Windows 创建对象时所基于结构的一个主要部分，与每个被访问的对象相关联，包含了安全对象的安全信息

包含的信息：标记（一组控制位集合）；所有者（拥有者或基本组对象的安全 ID）；自主访问控制列表 DACL；系统访问控制列表 SACL

访问控制列表（ACL）：Windows 访问控制机制的核心；当进程访问一个对象时，进程的 SID 将与对象的 ACL 进行比较，决定是否可以访问；附加到保护对象上的零个或多个访问控制项的顺序列表；每个访问控制项标识用户和组对该对象的访问权限

访问控制项（ACE），由对象的权限（拒绝访问、允许读取和写入、允许执行）以及用户或者组的 SID 组成

自主访问控制列表（DACL），决定了用户或组可以对该对象执行的操作

系统访问控制列表（SACL），描述了哪些类型的访问请求需要被系统记录，包含对象被访问的时间

审计事件类型：登录事件、账户登录事件、账户管理事件、对象访问、目录服务访问、特权使用、进程跟踪、系统事件、策略更改

日志文件：审计信息以二进制结构形式记录在磁盘文件中，包括事件名称、事件源、事件号、事件类别、机器名、用户名和事件本身的详细描述

系统日志

应用程序日志

安全日志

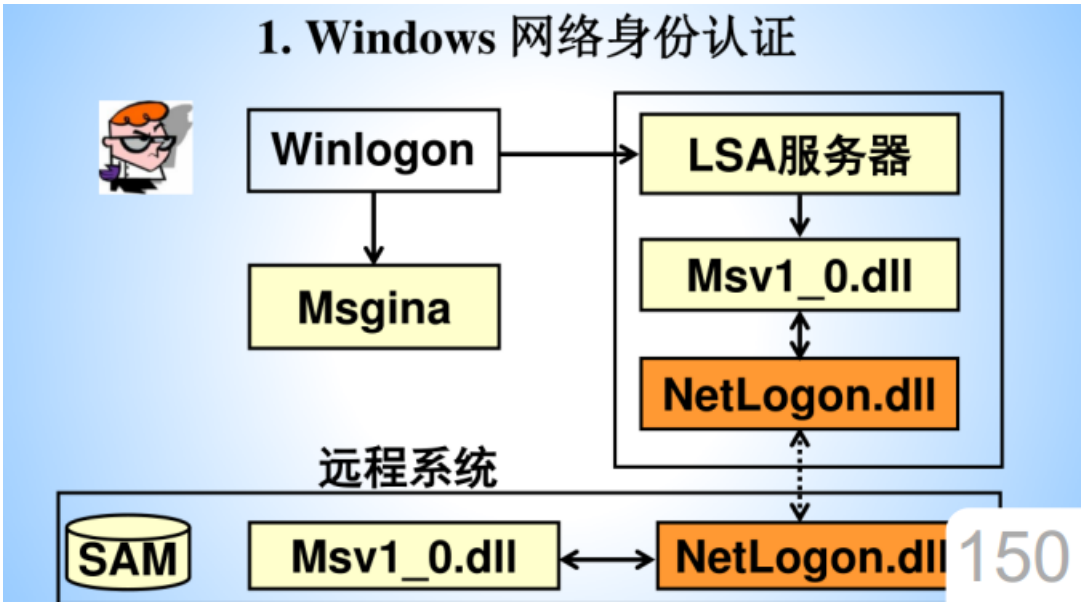
日志保护：禁止 Guest 访问

Windows 文件系统类型：FAT、NTFS；FAT 没有可靠性和兼容性，NTFS 分区支持自主访问控制和拥有权

加密文件系统 EFS，用于 NTFS 文件系统，使用户在本地计算机上安全存储数据；不能加密压缩和系统文件，加密后不能被共享，可以被删除、列出文件或目录

5.4 Windows 网络安全技术

网络身份认证



公钥基础设施（PKI），核心使微软证书服务系统

IP 协议的安全性，在设计和实现上存在安全漏洞，使各种攻击有机可乘

IPSec，通过使用加密安全服务，确保在 IP 网络上进行保密安全的通讯；IPsec 并不是一个单个的协议，而是能够在 IP 层提供互联网通信安全的协议族

IP 安全数据报格式的两个协议：鉴别首部（AH）协议，封装安全有效载荷（ESP）协议

在使用 AH 或 ESP 之前，先要从源主机到目的主机建立一条网络层的逻辑连接，即安全关联 SA（单向连接，传送 IP 安全数据报）

有关加密算法的三个协议

互联网密钥交换 IKE 协议

IIS，方便、易用，目前流行的 Web 服务器软件之一，但安全性。。。。

Windows 服务器的安全配置

使用 NTFS 文件系统，便于文件和目录管理

关闭默认共享

修改共享权限

为系统管理源账号更名，避免非法用户攻击，严禁非必要账号的创建和使用

禁用 TCP/IP 上的 NetBIOS

对进站连接进行控制（只允许 80 端口）

减小拒绝服务攻击的风险（修改注册表）

IIS 安全配置，安装、用户控制、登录认证、访问权限、IP 地址控制、转发安全、SSL 安全机制

防火墙

第六章 Linux 操作系统安全

6.1 Linux 安全概述

Linux 系统的启动过程：BIOS 加电自检>>加载主引导记录（MBR）>>加载操作

系统装载器>>加载 Linux 内核映像>>加载 init 进程
init 进程：执行文件为/sbin/init；Linux 中的所有进程都由 init 进程衍生，其进程号是 1；若 init 进程出现问题，系统中其他进程也会随之受影响
特权程序漏洞：特权程序是可以暂时获得管理源权限并执行一些管理员特权功能的程序；若程序执行流程被转到恶意代码上，即可使攻击者获得管理源权限
恶意代码：特洛伊木马往往取代系统登录程序或 ls，cp 等基本工具，在实现这些程序正常功能的同时，加入恶意代码
网络监听和数据捕获：通过截取网络数据，攻击者可以窃取远程登录的口令，截获传输的敏感信息，甚至通过篡改通信数据进行破坏活动
软件设置和相互作用：错误的软件设置可能会导致隐藏的安全问题；软件编写者可能无法准确预测软件各部分的相互作用，使软件在接收到一些非法参数时，可能出现意外的反应，例如使普通用户获得系统用户特权
安全机制：标识（UID，GID）；鉴别；访问控制；审计；网路安全防护

6.2 Linux 本地安全机制

用户和组安全

Linux 系统中文件和程序的访问控制以用户（UID）和用户分组（GID）为基础，保护用户和组管理安全非常重要

根用户（root）：系统的超级用户，拥有系统的最高权限

普通用户：由系统管理员创建的，可以登录系统，但只能操作自己拥有权限的文件；用户信息保存为普通文本文件，所有用户可读

系统用户配置文件/etc/passwd

用户影子文件/etc/shadow，只有 root 可读

系统组账号配置文件/etc/group

普通用户组口令安全存/etc/gshadow

Linux 系统核心支持多种文件系统类型

Ext，扩展文件系统

Ext2，支持自动修复损坏的文件系统和反删除

Ext3，不支持反删除

Ext4，使磁盘的 I/O 性能显著提高

Linux 系统基本的文件类型：普通文件；目录文件；设备文件；链接文件；管道文件

僵尸进程：一个进程调用了 exit 后，并非马上消失，而是留下一个称为僵尸进程的数据结构；僵尸进程放弃了几乎所有内存空间，无任何可执行代码，也不能被调度，仅仅在进程表中保留一个位置，记载该进程的退出状态等信息供其他进程收集；如果存在太多僵尸进程会占用内存资源，影响系统性能和新进程的产生，甚至导致系统瘫痪

Linux 日志管理，主要用于监测和审计

Syslog 机制，进行系统日志的管理和配置，由守护进程/etc/syslogd、配置文件/etc/syslog.conf

6.3 Linux 网络安全技术

Web 服务安全

配置特定的用户运行 Apache 服务器

服务器配置隐藏 Apache 服务器 httpd 主配置文件 http.conf

访问控制

使用认证和授权保护
设置虚拟目录
Apache 服务器的安全模块
应用 SSL 技术
Netfilter/Iptables 防火墙：包过滤，NAT，数据报处理
五链：prerouting、input、output、forward、postrouting
四表：filter、nat、mangle、raw
入侵检测，Snort，有嗅探器、数据包记录器、网络入侵检测系统三种工作模式
DNS 服务安全的安全措施：配置辅助域名服务器，配置高速缓存服务器，负载均衡，配置 DNS 查询方式，DNSSEC 安全防护
DHCP 服务安全：系统自带的 rpm 包，dhcpd 软件，chroot 机制
网络服务管理程序：存取控制，Dos 攻击防御，日志功能，请求转发，IPv6，与客户端交互

第七章 数据库系统安全

7.1 数据库系统安全概述

数据库管理系统（DBMS）
组成：主要包括存储管理器和查询处理器
功能：建立、管理和维护数据库；为用户及程序提供数据访问；保证数据库的安全性
数据库系统安全威胁源分类：自然灾害，设备故障，人为疏忽，恶意攻击，管理漏洞

7.2 数据库系统的安全需求

机密性：数据值；可能的取值；数据值的范围；否定的查询结果
完整性：防止对 DBMS 的非法访问和修改；保护存储的数据、文件的安全性
数据的完整性：物理数据库完整性；逻辑数据库完整性；元素完整性
一致性：表示同一事实的两个数据应相同；满足某一约束关系的一组数据不应该发生互斥
可审计性：数据库受破坏后可恢复，维护完整性；防止用户采用累加的方式，访问受保护的数据；审计、跟踪用户访问记录，推理用户意图
两阶段更新：准备阶段，提交阶段
数据库系统的安全防护层次：数据库系统安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、操作人员素质等因素息息相关，其安全防护可分为四个层次
网络环境层次：数据库系统的安全首先依赖于网络系统，网络系统的安全使数据库系统安全的第一道屏障
宿主操作系统层次：防止对 DBMS 的非法访问和修改；保护存储的数据、文件的安全性；对数据库用户进行系统登录认证
数据库管理系统层次：保护数据的机密性、完整性、一致性、可用性；并发控制
数据库应用系统层次：用户管理，身份认证，用户/角色管理，访问控制，业务审计，输入检查；SQL 注入攻击最基本的防范——不允许输入符号'，将输入的符号'转换

7.3 数据库系统的安全机制

视图机制

原理：通过定义不同的视图，将用户无权访问的数据隐藏起来

实现：创建视图，授予用户指定视图的查询权限

数据库加密

库外加密：加解密过程发生在 DBMS 外，DBMS 管理的是密文

优点：对 DBMS 要求少；缺点：数据加解密需要很大的时间和空间

库内加密：加密对象为数据库中存储的数据；在 DBMS 内核层实现加密，加解密过程对用户与应用透明，数据在物理存取之前完成加解密工作

优点：加密的粒度可细化，效率较高；缺点：DBMS 性能降低，密钥管理风险较大

局限性：不宜以整个数据库文件为单位进行加密；部分字段不能加密

推理控制，攻击者利用数据之间的相互关系，从合法获得的低安全等级的数据中，推导出数据库中受高安全等级保护的内容，从而造成敏感信息的泄露

7.4 SQL Server 数据库安全

操作系统级的安全防线——OS 身份认证和访问控制

服务器级的安全防线——SQL Server 身份认证

数据库系统级的安全防线——特定数据库自己的用户账户和角色

数据库对象级的安全防线——用户必须在自己的权限范围内操作数据

Windows 身份认证模式/混合身份认证模式

SQL Server 账号安全性检查：检查无用的数据库账号，检查弱口令账号，检查空口令账号

权限管理

语句权限（创建对象的权限）

SQL Server 的存储过程：SQL 服务器上的一组预编译好的可以完成特定功能的 SQL 语句集，可分为系统存储过程、自定义存储过程两种

对象权限（操作对象的权限）

表或视图；存储过程；内嵌表值函数；表或视图的列

隐含权限（通过角色传递得到的权限）

将用户加入角色，系统自动将角色的权限传递给成员

入侵检测

系统日志：数据库服务停止或重新启动，执行扩展存储过程记录

数据库管理系统日志：多次登录失败记录，数据库登录日志

数据库应用日志：执行插入的 SQL 语句，检查用户输入的符号是否对系统有威胁

数据控制

完整性控制：主要体现在 CREATE TABLE 语句，在该语句中定义约束条件

并发控制：多个操作时采用封锁机制，以保证操作的正确性和数据库的一致性

数据恢复：处于不一致状态时具备恢复到一直状态的功能；SQL 语言支持事务、提交、回滚等概念

安全性控制：保护数据库，防止不合法的使用造成数据泄露和破坏；主要是对用户进行授权和访问控制

存储过程管理：限制用户的权限，只授予其执行存储过程的权限；用户只能

通过存储过程来访问表，从而保证数据的安全性

第八章 信息系统安全测评

目的和意义：科学分析并确定风险的过程；信息安全建设的起点和基础；需求主导和重点原则的具体体现；组织机构实现信息系统安全的重要步骤

信息系统安全的 5 个等级

用户自主保护级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益

系统审计保护级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全

安全标记保护级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害

结构化保护级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害

访问验证保护级：信息系统受到破坏后，会对国家安全造成特别严重的损害

定级要素：等级保护对象受到破坏时所侵害的客体；对客体造成侵害的程度

相关概念

资产：组织中具有一定价值，需要保护的资源

资产价值：资产的属性，指明资产的重要程度和敏感程度；根据资产损失所引发的潜在业务影响来决定

威胁：有可能引起安全事件的，会对组织级资产造成直接或间接损害的潜在因素

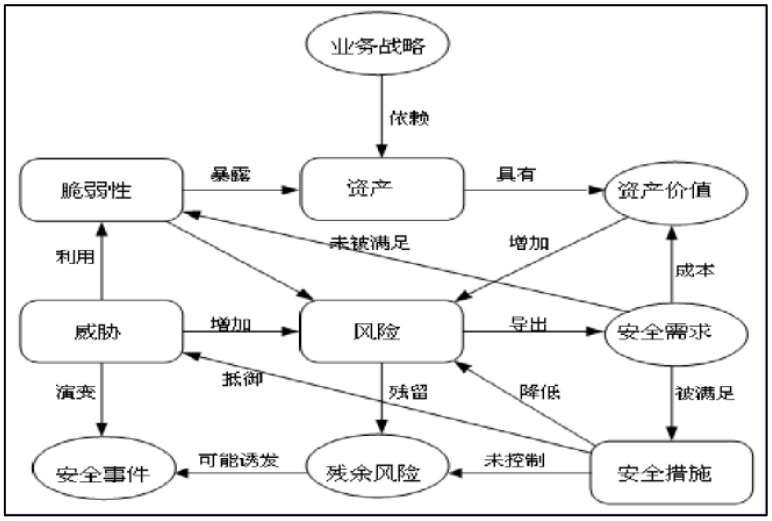
脆弱性（漏洞）：资产的弱点；可能被威胁利用造成安全事件发生，引起资产遭受损害

风险：使得威胁可以利用脆弱性，从而直接或者间接造成资产损害的一种潜在的影响

风险评估：对威胁、脆弱性、影响及三者发生的可能性评估，确定资产的风险等级和确定有限控制顺序的过程

安全控制：用来保护组织资产，防止威胁，减少脆弱性，限制事件影响的安全实践、过程和机制

信息安全风险管理各要素间的关系



信息安全风险评估的原则

可控性原则：人员、工具、项目过程

完整性原则：应严格按照委托单位的评估要求和指定的范围进行全面的评估服务

最小影响原则：从项目管理层面和工具技术层面，力求将风险评估对系统正常运行的可能影响降到最低

保密原则：与评估对象签署保密协议和非侵害性协议，要求参与评估的单位或个人对评估过程和结果数据严格保密，未经授权不得泄露给任何企业和个人

第九章 可信计算

9.1 可信计算概述

可信计算的出发点：提供一种方法使实体能够判断与其交互的实体是否可信，确保网络空间中交互的安全

可信计算系统是能够提供系统可靠性、可用性、信息和行为安全性的计算机系统

9.2 可信计算机系统的组成和技术原理

信任根：系统可信的基点，TCG 认为一个可信计算平台必须包括可信测量根、可信存储根、可信报告根 3 个信任根

信任链把信任关系从信任根扩展到整个计算机系统

可信硬件平台

可信操作系统

可信应用系统

基本思想：先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，把这种信任扩展到整个计算机系统，并采取防护措施，确保计算机资源的完整性和行为的预期性，从而提高计算机系统的可信性

可信计算平台对请求访问的实体进行可信测量，并存储测量结果，实体询问时平台提供报告

9.3 可信计算技术的应用

应用领域：电子商务、安全风险管理、数字版权管理、安全监测与应急响应、国防等领域

计算机、服务器、网络产品

支持可信计算的操作系统