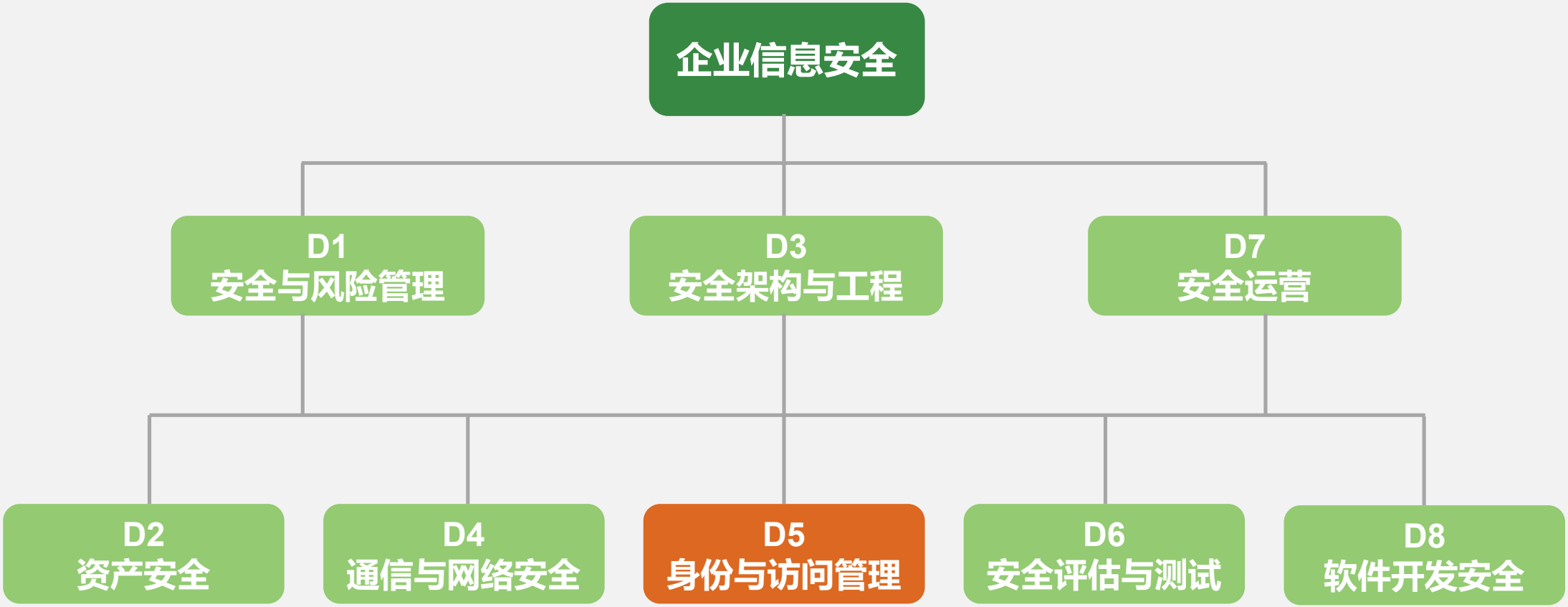
铭学在线课堂-CISSP认证

D5：身份与访问管理

铭记初心，实现自我

知识架构



CBK学习目标

- 对身份管理系统、单一和多因素身份认证、可追溯性、会话管理，身份注册与证明、联合身份管理和凭证管理系统等知识的掌握情况。
- 实施和管理授权机制，包括基于角色、基于规则的访问控制，强制访问控制和自主访问控制。

本章知识架构

本节目标

1.1 基本概念

- A、相关定义
- B、四个要素

相关术语

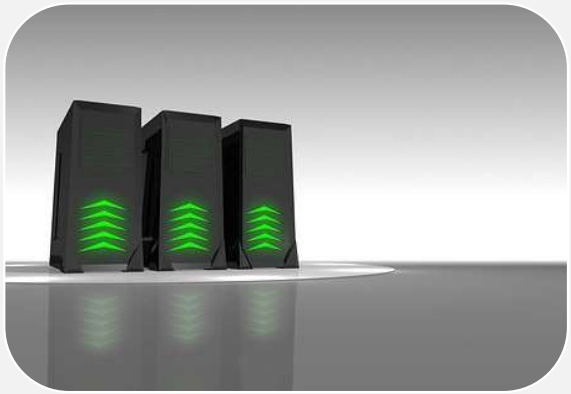
- 主体与客体
- 访问是在主体和客体之间进行的信息流动
- 访问控制是一种安全手段，它控制用户和系统如何与其他系统和资源进行通信和交互
- 访问控制包含的范围很广，它涵盖了几种对计算机系统、网络和信息资源进行访问控制的不同机制
- 访问控制是防范计算机系统和资源被未授权访问的第一道防线

目标和原则

相关分类

- 访问控制由3个大的类别组成：

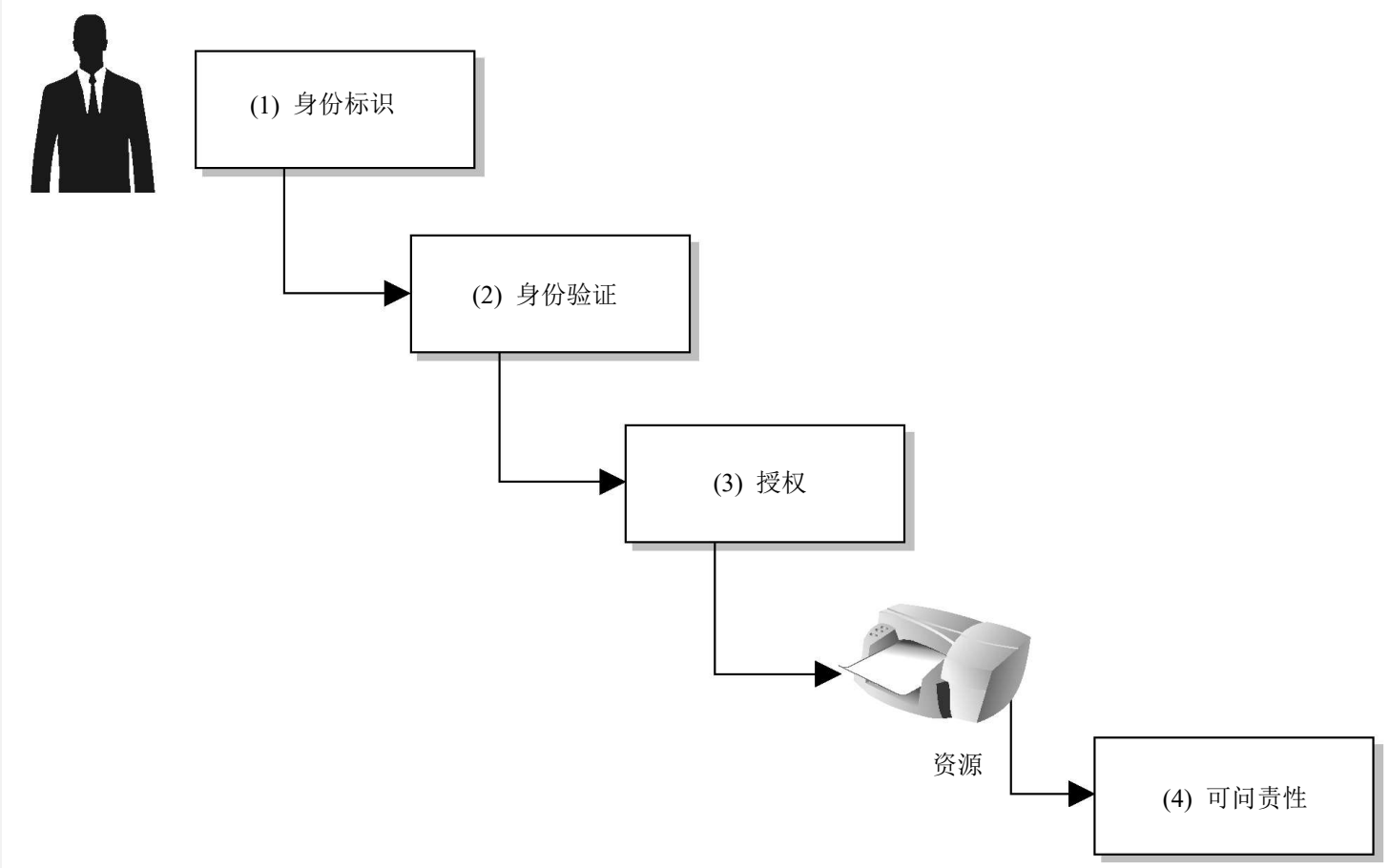
行政管理性



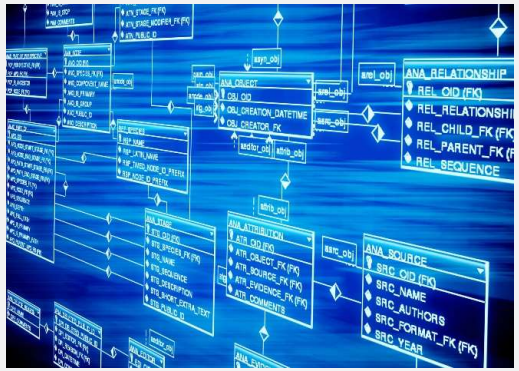
技术性

物理性

四个要素



竞态条件



本节目标

1.2 标识和认证

- A、身份标识
- B、身份验证因素
- C、密码
- D、智能卡和令牌
- E、生物识别技术

身份标识

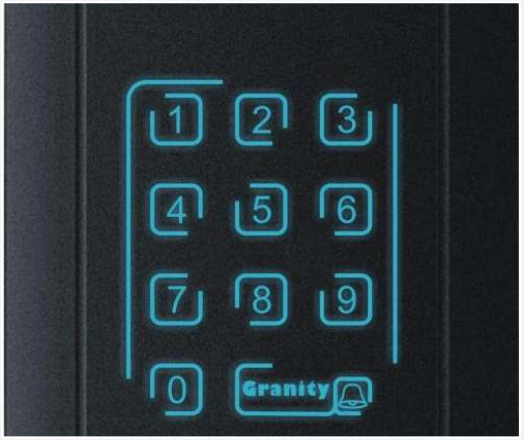
- 身份标识是所有访问控制的起点
- 没有正确的身份标识，就无法确定如何进行适当的控制
- 身份标识应该确保：
  - ✓ 每个值应当是唯一的，便于用户问责
  - ✓ 应当遵循一个标准的命名方案
  - ✓ 身份标识值不得描述用户的职位或任务
  - ✓ 身份标识值不得在用户之间共享

身份验证因素

- 一般来说，有下列3种因素能够用于身份验证：
  - ✓ 某人知道什么
  - ✓ 某人拥有什么
  - ✓ 某人是什么
- 多因素身份验证
- 其它一些验证方式

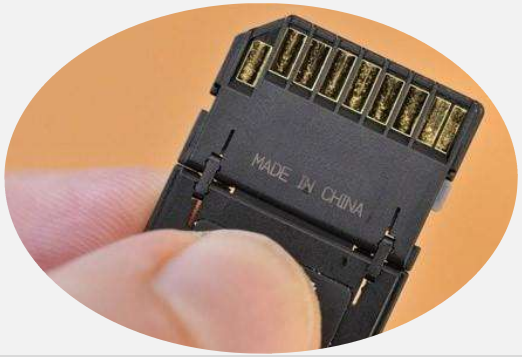
密码

- 类型1的认证方式
- 密码管理
- 针对密码的攻击
- 针对密码管理攻击的安全措施
- 使用感知密码、密码短语和一次性密码来增加安全性。



存储卡、智能卡和令牌

- 存储卡、智能卡和令牌都是类型2身份验证因素(或者你拥有什么)
- 存储卡与智能卡的主要差异在于处理信息的能力
- 同步动态密码令牌和异步动态密码令牌
- 相关攻击



生物测定学

- 类型3的认证方式
- 生理性生物测定和行为性生物测定
- 误报(false positive)和漏报(false negative)
- 指纹、手掌扫描、手部外形、虹膜扫描、动态签名、动态击键、声纹、面部扫描、手形拓扑
- 生物测定学的问题

本节目标

1.3 授权和可问责性

- A、权限、权利和特权
- B、授权机制和原则
- C、可问责性

权限、权利和特权

- 权限(permission) 通常是指授予主体对客体的访问权限，并确定主体可对其执行的操作。
- 权利(right) 主要是指对某个客体采取行动的能力
- 特权(privilege)是权利和权限的组合

授权机制和原则

- 网络管理员和安全专家在进行保护配置时希望能够对资源进行充分的控制，而且对每一个用户都进行非常准确的控制
- “知其所需”准则，个人应当只被允许访问为履行其职责而需要的信息
- 为了满足了“知其所需”准则，可以对各种角色、组、位置、时间和事务处理类型实施不同的访问准则

授权机制和原则

- 最小特权原则确保主体仅被授予执行其工作任务和工作职能所需的权限。这通常会和“知其所需”原则混淆。唯一的区别是最小特权还包括对系统采取行动的权利。
- 授权蠕动，当雇员在一家公司长期工作时，他们会从一个部门调动到另一个部门，因此常常被赋予越来越多的访问权限和许可

授权机制和原则

- 职责分离原则确保将敏感职能分为两个或多个员工执行的任务。通过创建一个检查和制衡系统来防止欺诈和错误
- 访问控制机制应当默认拒绝访问，以实现必要的安全级别并确保没有被忽略的安全漏洞

可问责性概述

- 审计功能确保用户的动作可问责，验证安全策略已实施，并且能够用作调查工具
- 我们通过记录用户、系统和应用程序的活动来跟踪可问责性
- 审计跟踪还可用于提供有关任何可疑活动的报警，从而方便之后的调查

审计日志和审查方法

- 在发生安全违规、无法解释的系统活动或系统崩溃后，审计日志是非常重要的检查项
- 自动工具和手工审查
- 安全信息和事件管理(Security Information and Event Management，SIEM)

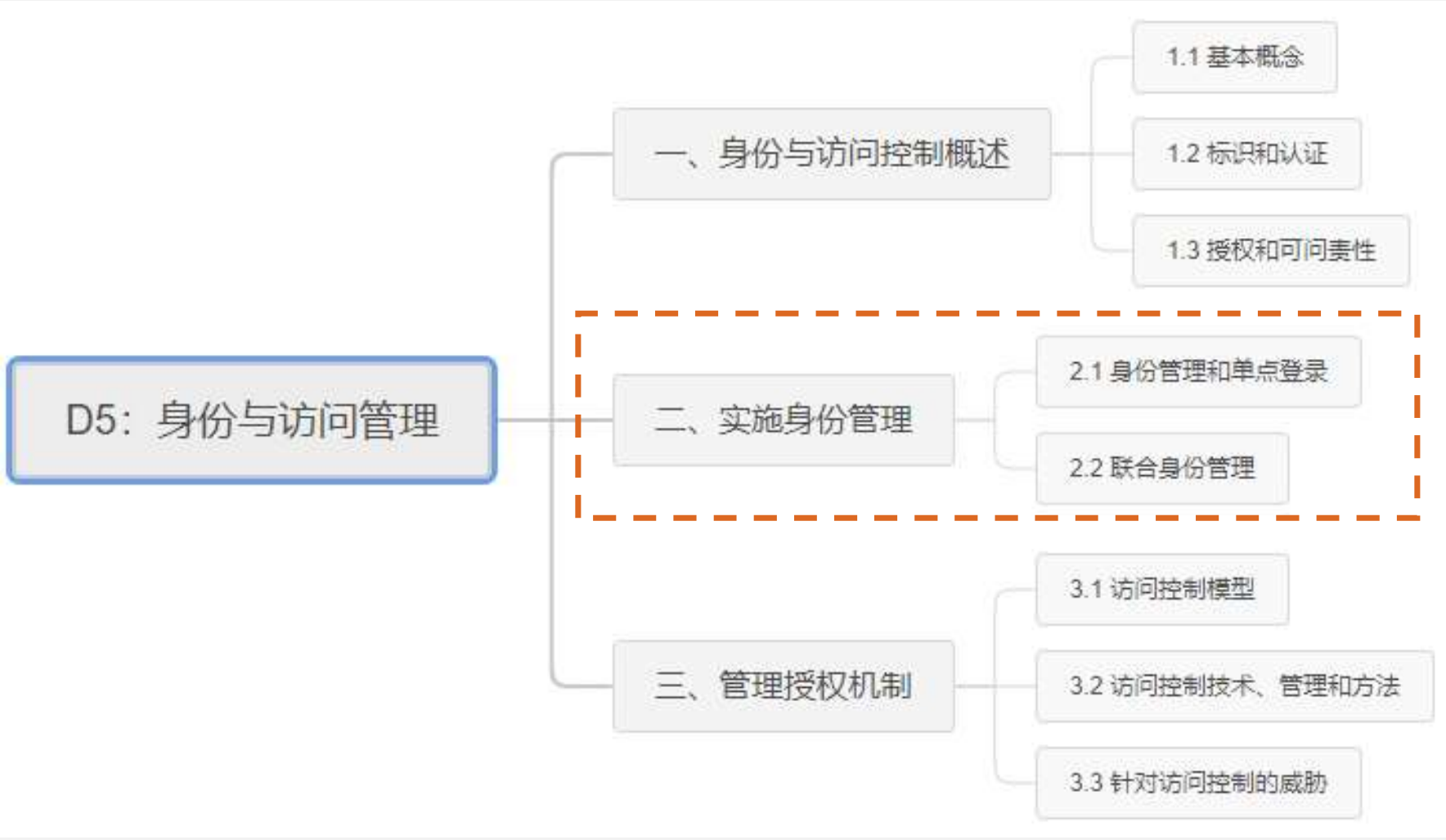
保护审计数据和日志信息

- **擦洗(scrubbing)：**攻击者经常会删除保存其犯罪活动信息的审计日志
- 应当采用严格的访问控制对审计日志加以保护，采用适当的步骤来保证审计信息的机密性和完整性不会受到任何形式的破坏
- 应当只有特定的人（管理员和安全人员）才能够查看、更改和删除审计跟踪信息

击键监控

- 击键监控是一种能够检查和记录用户在操作过程中的键盘输入的监控行为
- 使用这种监控的人可以将用户输入的字符写入审计日志，以备日后检查
- 黑客也可以利用这种监控
- 这种监控往往会涉及隐私问题，公司应当采取这些步骤来保证不会侵犯个人的隐私，同时应向用户通告与计算机使用有关的隐私界限

本章知识架构



本节目标

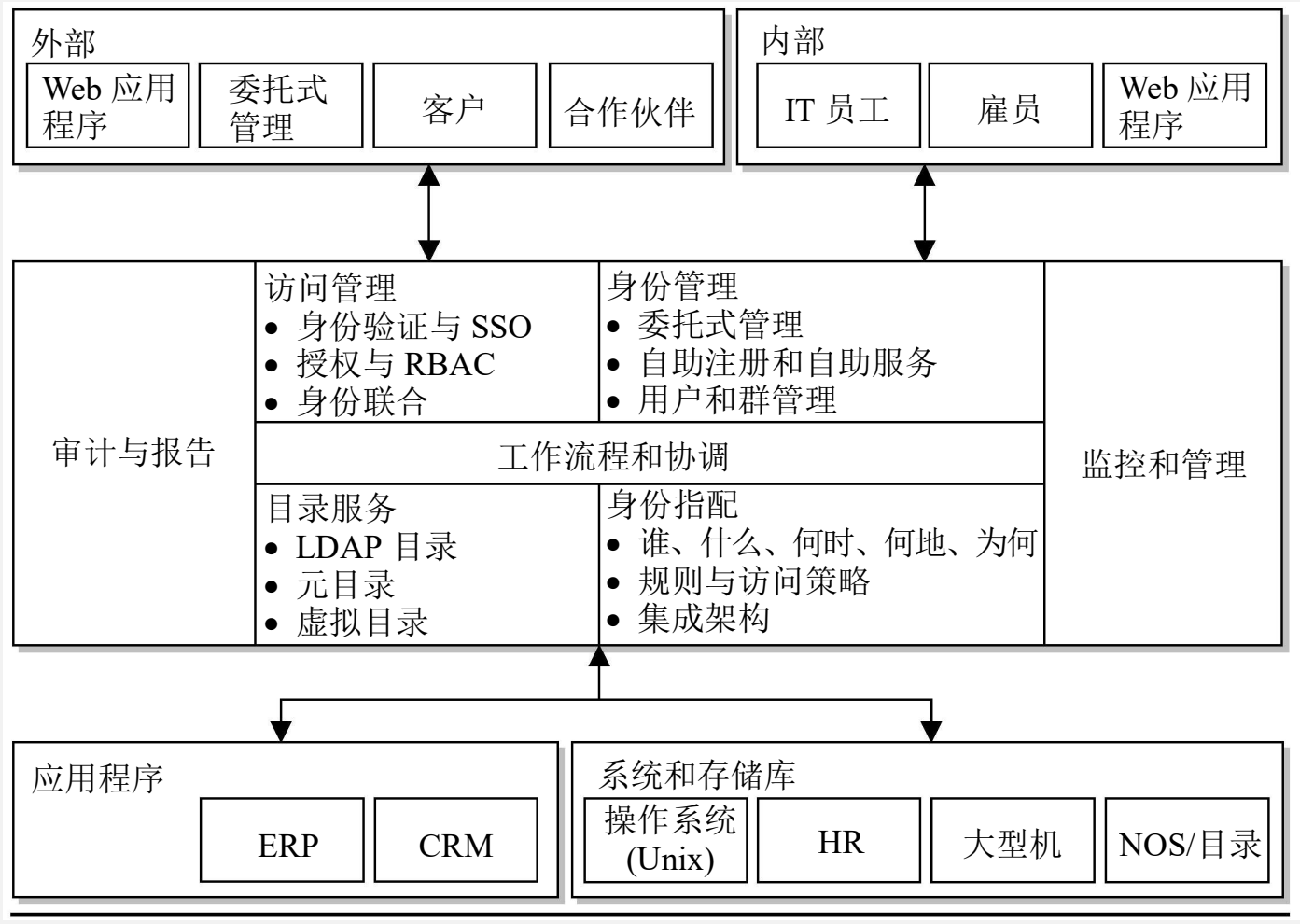
2.1 身份管理和单点登录

- A、身份管理
- B、单点登录
- C、管理身份和访问配置生命周期

身份管理

- 身份管理(Identity Management，IdM)是一个广泛而又深入的术语，包括使用不同产品对用户进行自动化的身份标识、身份验证和授权
- 企业目前在控制资产访问方面需要处理的许多常见问题
- 市面上有许多身份管理解决方案和产品

身份管理

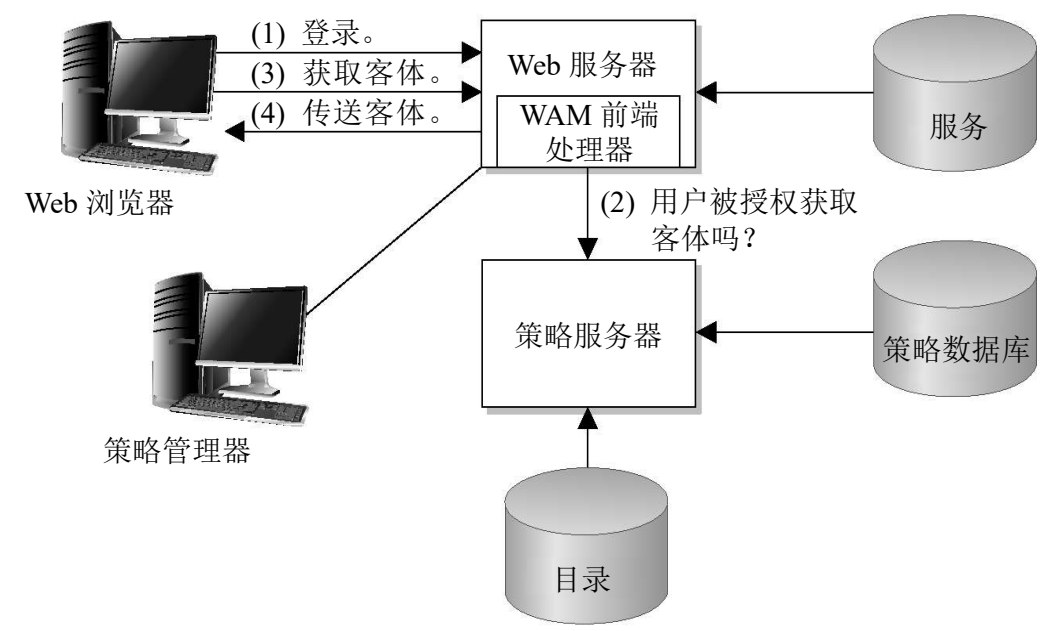


身份管理

- 大多数企业都使用某种类型的目录，目录中包含了与公司网络资源和用户有关的信息
- 目录内的客体由目录服务管理
- 目录服务如何让这些实体保持有序运行呢?
- 目录在身份管理中的角色是什么呢?
- 常见的目录协议：X.500 LDAP 微软域（AD）管理

身份管理

- Web访问管理（Web Access Management，WAM）软件用于控制用户在使用Web浏览器与基于Web 的企业资产进行交互时能够访问哪些内容

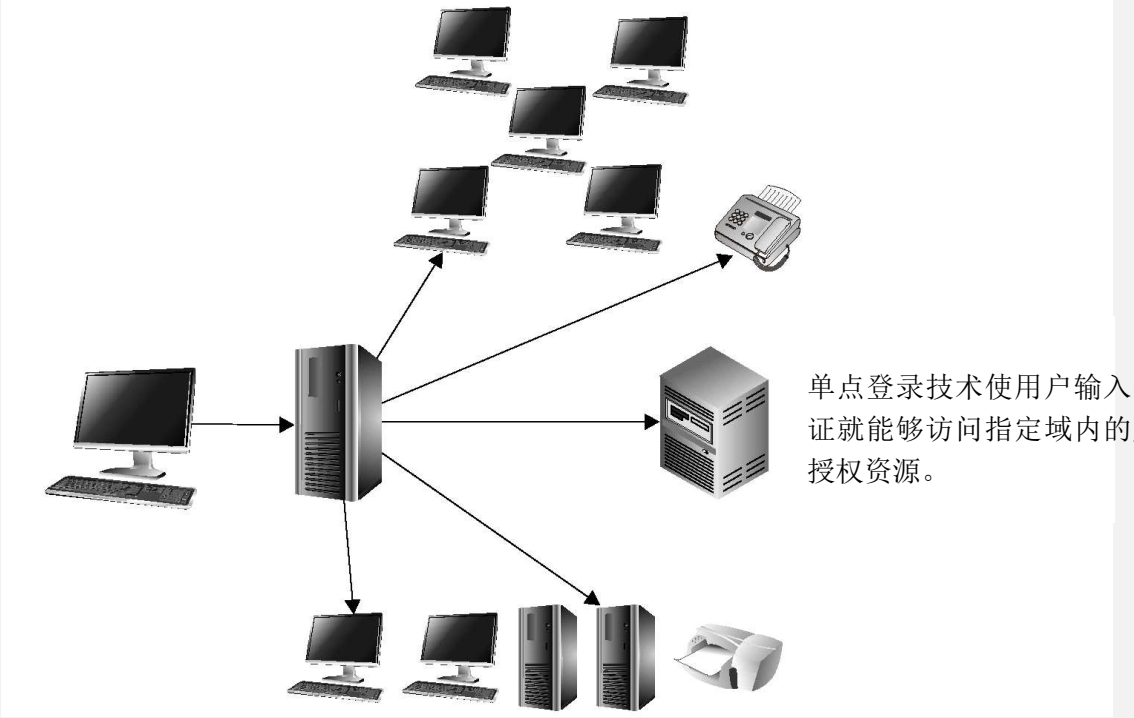


身份管理

- 一些最常用的密码管理方法：
  - ✓ 密码同步
  - ✓ 自助式密码重设
  - ✓ 辅助式密码重设

单点登录

- 单点登录（SSO），允许用户只输入一次凭证，就能够访问主网络域和辅助网络域中的所有资源



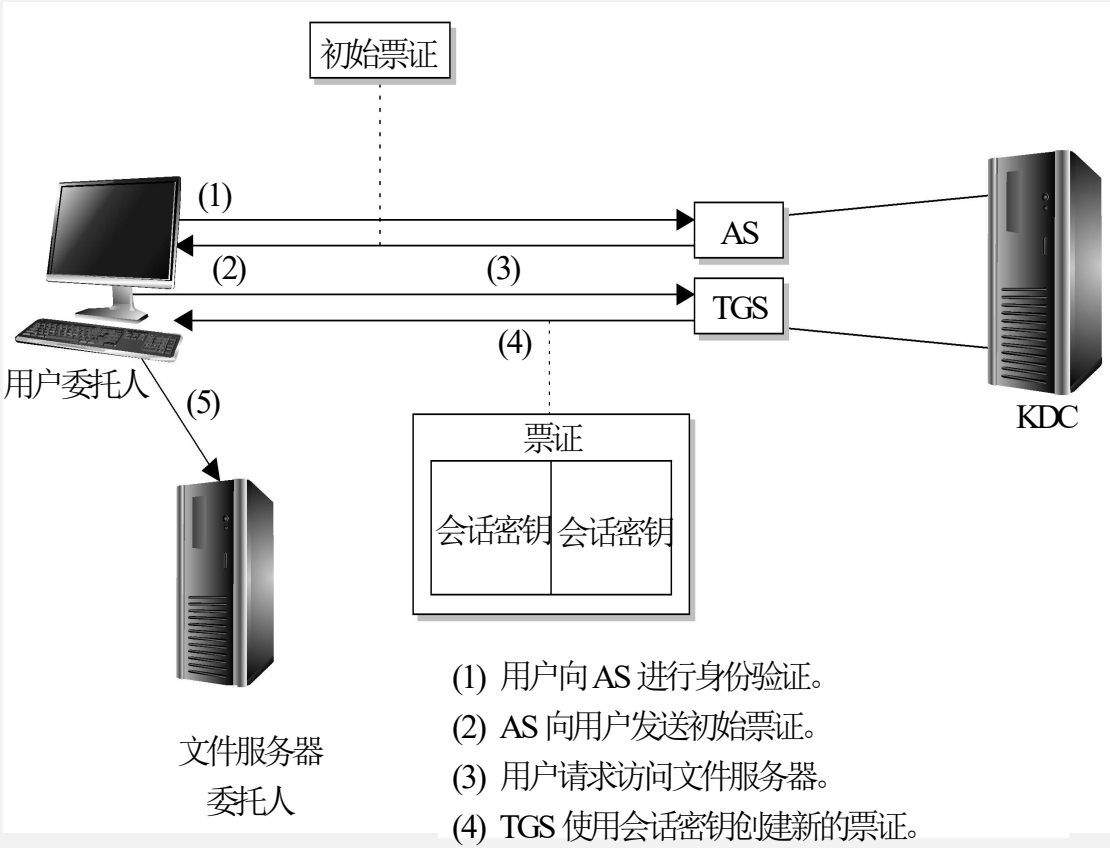
单点登录技术使用户输入一次凭证就能够访问指定域内的所有预授权资源。

单点登录

- 单点登录技术的示例
  - ✓Kerberos 使用KDC和票证的身份验证协议，基于对称密钥密码学。
  - ✓SESAME 使用PAS和PAC的身份验证协议，基于对称和非对称密码学。
  - ✓安全域 在相同安全策略下运行的资源，由相同的组管理。
  - ✓目录服务 允许资源以标准化方式命名和允许访问控制被集中维护的一种技术。
  - ✓瘦客户端 依赖一台中央服务器进行访问控制、处理和存储的终端。

单点登录

- Kerberos协议
- 一个身份验证协议
- 分布式环境中单点登录的一个示例
- 异构网络的一个实际标准



管理身份和访问配置生命周期

- 身份和访问配置生命周期是指账户的创建、管理和删除
- 访问控制管理是在账户生命周期中，管理账户、访问和问责所涉及的任务和职责的集合
- 三个主要职责：配置、账户审核和账户撤消。

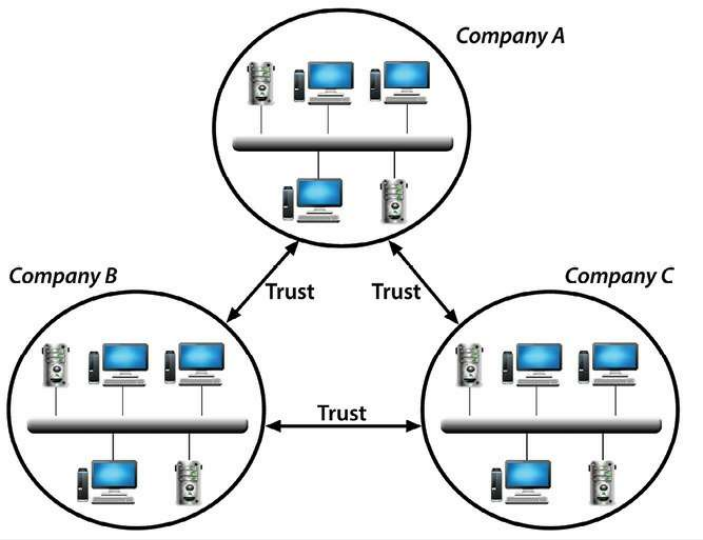
本节目标

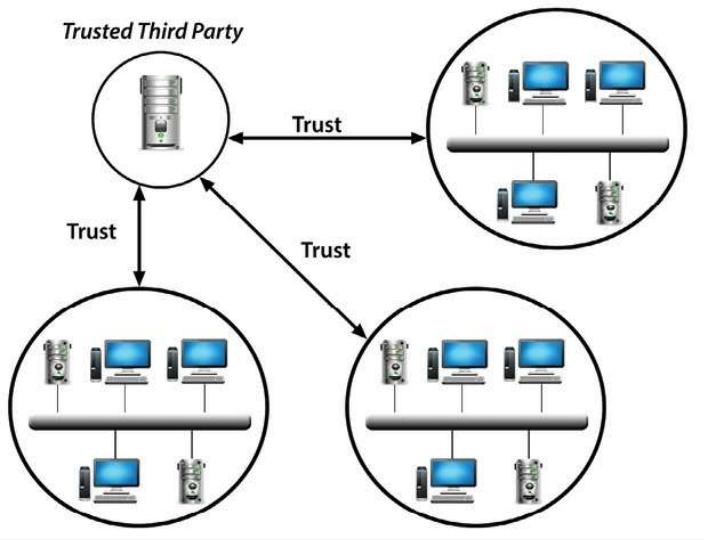
2.2 联合身份管理

- A、联合身份管理概述
- B、SAML、SPML和XACML
- C、OAuth 2.0
- D、OpenID和OpenID连接
- E、IDaaS

联合身份管理概述

- 身份管理是用户身份及其凭据的管理
- 联合身份管理（FIM）将其扩展到单一组织之外
- 两种模式：交叉认证模式和可信第三方模式



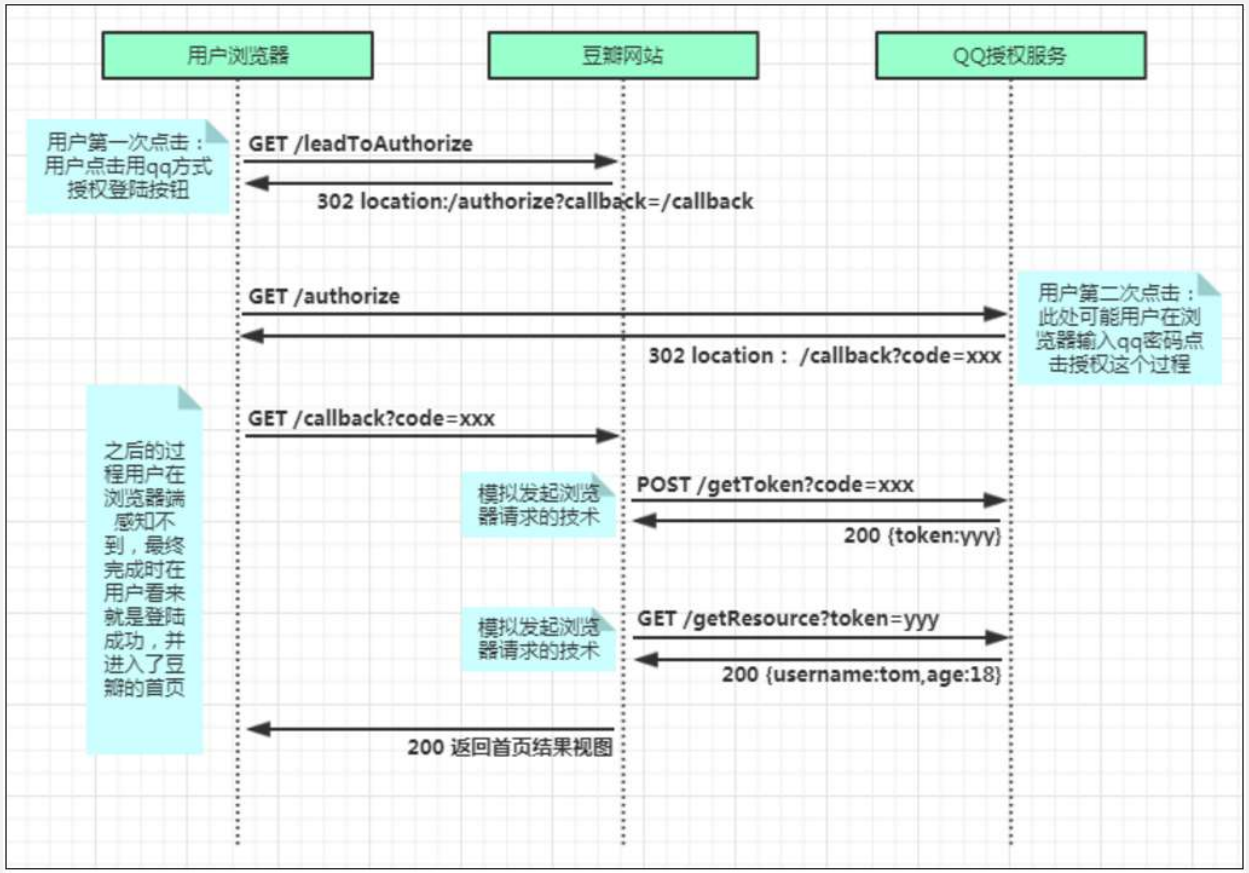


SAML、SPML和XACML

- 安全断言标记语言 (SAML)是一种基于XML的语言，通常用于在联合组织之间交换身份验证和授权(AA)信息
- 服务配置标记语言(SPML)是由OASIS开发的一种新框架，它基于XML，专门用来交换用于联合身份SSO目的的用户信息
- 可扩展访问控制标记语言(Extensible Access Control Markup Language，XACML)是由 OASIS开发的标准，用于定义XML格式的访问控制策略

OAuth

- OAuth（开放授权）是对第三方的一个开放授权标准（非身份验证）



OpenID和OpenID连接

- OpenID（开放式认证系统）是由第三方进行用户身份验证的开放标准
- OpenID连接是使用OAuth 2.0框架的身份验证层

身份即服务IDaaS

- 身份即服务（Identity as a Service，IDaaS）是一种软件即服务（SaaS），通常联合IdM和密码管理服务，并被配置用于提供单点登录（SSO）
- 一些受监管的行业可能无法利用IDaaS并保持兼容
- 一些最关键的数据将会更多地被暴露
- 整合的问题

本章知识架构

本节目标

3.1 访问控制模型

- A、实施纵深防御和模型概述
- B、自主访问控制
- C、强制访问控制
- D、基于角色的访问控制
- E、基于规则的访问控制
- F、基于属性的访问控制

实施纵深防御和模型概述

- 纵深防御策略：使用多个层级的访问控制来提供分层安全性。
- 纵深防御的概念突出了几个重点:
  - ✓组织的安全策略
  - ✓人员
  - ✓管理、 技术和物理访问控制的组合

实施纵深防御和模型概述

- 访问控制模型是规定主体如何访问客体的一种架构
- 访问控制模型主要有下列3种：

自主访问控制

强制访问控制

角色访问控制

自主访问控制模型

- 自主访问控制（DAC）：
  - ✓ 资源的所有者能够指定哪些主体可以访问该资源
  - ✓ 基于为用户授予的授权限制访问
  - ✓ 如所有的Windows、Linux和OS X系统以及主流的Unix系统

强制访问控制模型

- 强制访问控制（MAC）：
  - ✓ 在基于MAC 模型的多数系统中，用户不能安装软件、改变文件许可级别和添加新用户等
  - ✓ 更为结构化、更为严格，并且基于安全标签系统
  - ✓ 安全许可和分类数据存储在安全标签内，安全标签则绑定在特定的主体和客体上
  - ✓ 根据主体的安全许可、客体的分类以及系统的安全策略来做出决策

角色访问控制模型

- 角色访问控制（RBAC）模型：
  - ✓ 使用集中管理的控制方式来决定主体和客体如何交互
  - ✓ RBAC方式允许根据用户的工作角色来管理权限，从而简化了访问控制管理
  - ✓ RBAC模型是雇员流动性高的公司最适合使用的访问控制系统

规则型访问控制模型

- 规则型访问控制使用特定的规则来规定主体和客体之间可以做什么，不可以做什么
- 建立在传统的RBAC之上，因此通常也被称为规则型RBAC（RB-RBAC）

基于属性的访问控制

- 访问控制(ABAC)模型使用包含规则的多个属性的策略
- 属性可以是用户、网络和网络上的设备的任何特征

访问控制模型的总结

- 数据所有者决定谁能访问资源，ACL用于实施安全策略

DAC

- 操作系统通过使用安全标签来实施系统的安全策略

MAC

- 访问决策基于主体的角色和/或功能位置

RBAC

- 把进一步限制访问决策的强加规则添加到RBAC中

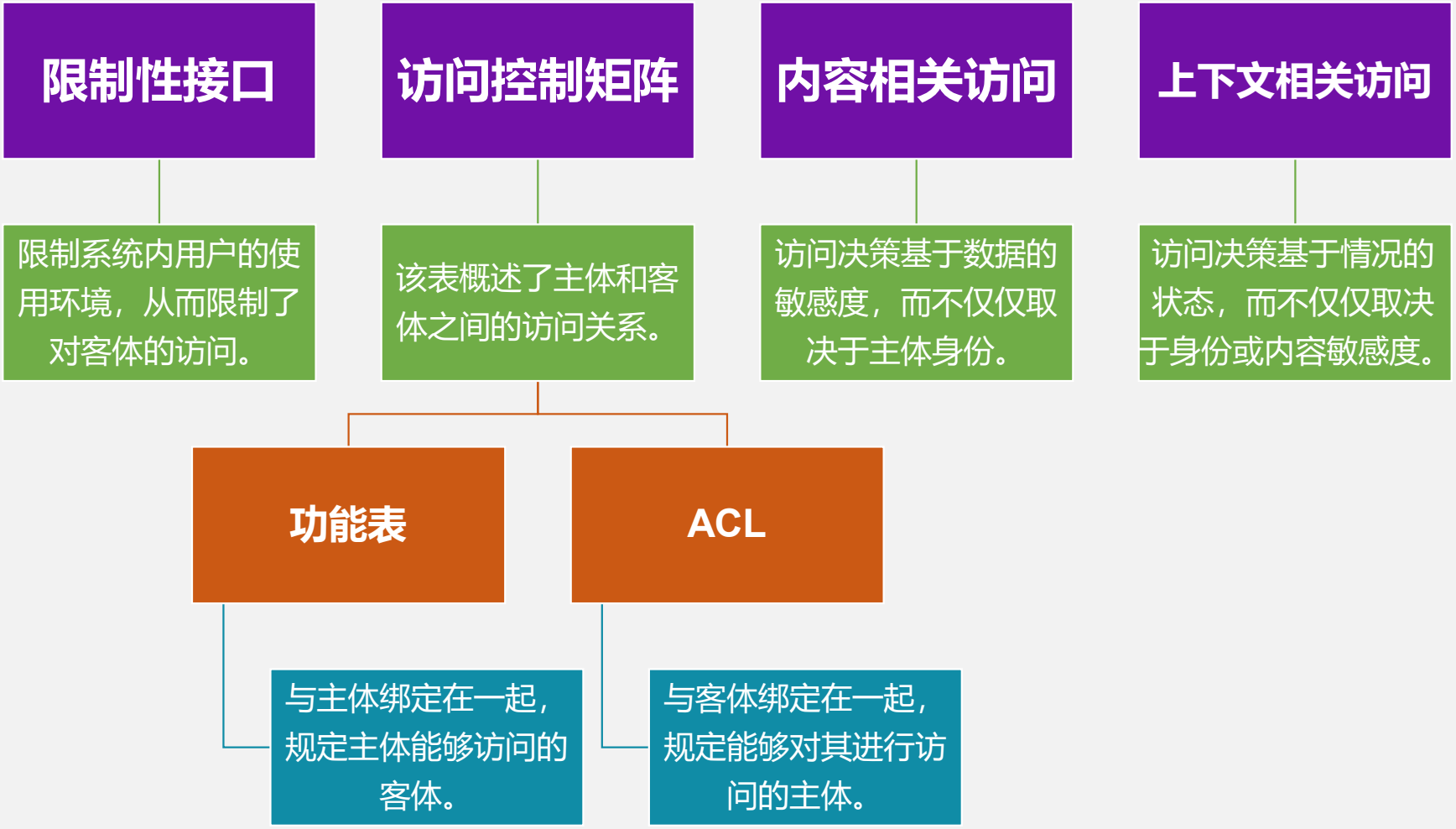
RB-RBAC

本节目标

3.2 访问控制技术、管理和方法

- A、访问控制技术
- B、访问控制的管理和方法

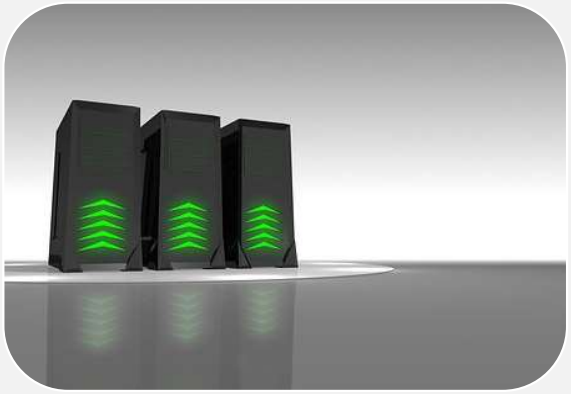
访问控制技术



访问控制实现方法

- 访问控制实现方法由3个大的类别组成：

行政管理性

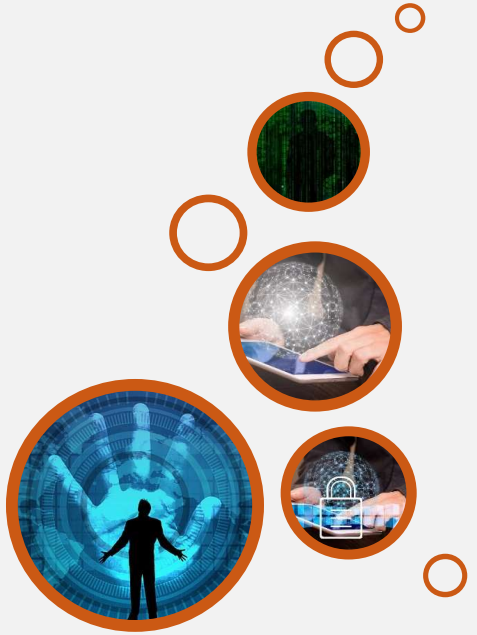


技术性

物理性

访问控制管理

- 集中式访问控制管理
  - RADIUS
  - TACACS
  - Diameter
- 分散式访问控制管理
  - 将访问的控制权交给资源附近的人员，也就是最清楚谁应该以及谁不应该访问这些文件、数据和资源的人。



本节目标

3.3 针对访问控制的威胁

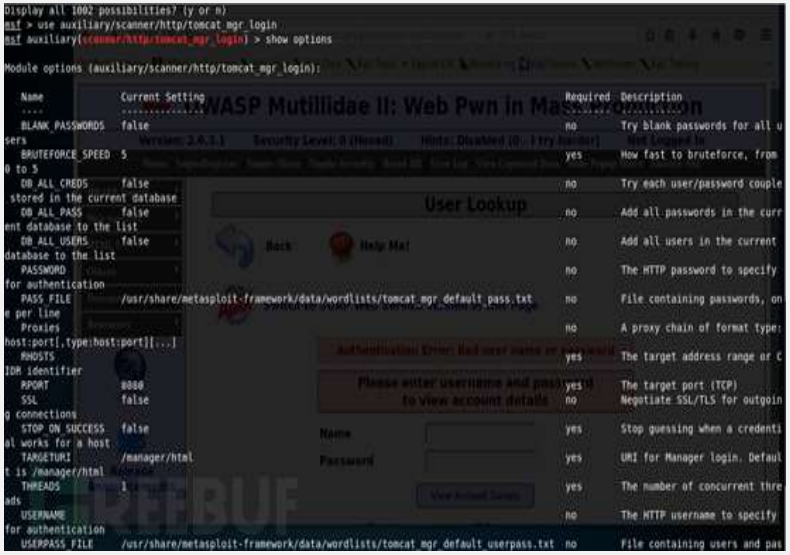
- A、访问聚合攻击
- B、密码攻击
- C、生日攻击
- D、欺骗攻击
- E、社会工程学
- F、网络钓鱼
- G、智能卡攻击
- H、相关防御措施

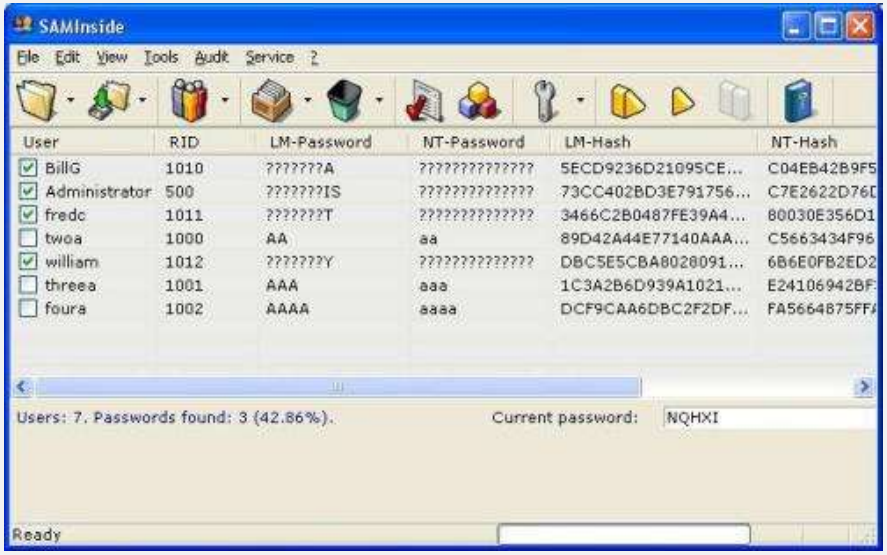
访问聚合攻击

- 访问聚合是指收集多条非敏感信息并将它们组合(即聚合)以获得敏感信息
- 侦察攻击是一种访问聚合攻击

密码攻击

- 密码是最弱的身份验证形式
- 使用字典、暴力、彩虹表和嗅探方法的常见密码攻击





生日攻击

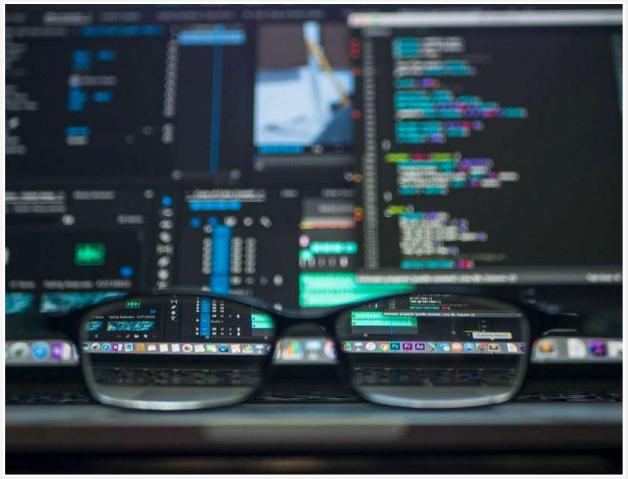
- 生日攻击的重点是寻找碰撞
- 生日攻击名称来自一个被称为生日悖论的统计现象

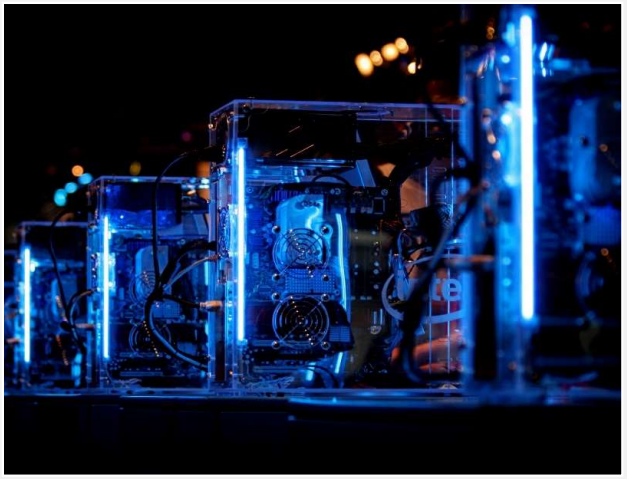
欺骗攻击

- 欺骗(也称为伪装)假装成某种东西或某个人
- 电子邮件欺骗、IP欺骗和电话号码欺骗

社会工程学

- 社会工程学是一种利用人的弱点如人的本能反应、好奇心、信任、贪便宜等弱点进行
- 诸如欺骗、伤害等危害手段，获取自身利益的手法。





网络钓鱼(phishing)

- 是一种社会工程攻击，其目标是获取个人信息、凭证、信用卡号或财务数据
- 鱼叉式网络钓鱼\捕鲸式钓鱼
- 网址嫁接

智能卡攻击

- 智能卡提供比密码更好的身份验证，特别是多因素使用时
- 侧信道攻击是一种被动的非侵入性攻击， 旨在观察设备的操作

相关防御措施

- 控制对系统的物理访问
- 控制对文件的电子访问
- 创建强密码策略
- 散列和加盐密码
- 使用密码屏蔽
- 部署多因素身份验证
- 使用账户锁定控制
- 使用上次登录通知
- 用户安全培训


THANK YOU
感谢聆听
以科学方法推动IT新职业发展