第十三章 管理身份与认证

13.1 控制对资产的访问

- 资产可以包括信息、系统、设备、设施和人员

13.1.1 主体与客体的对比

13.1.2 访问控制的类型

- 访问控制时所有控制访问资源相关的硬件、软件或管理类策略或程序，目标是向授权主体提供访问并阻止任何未经授权的蓄意访问
- 访问控制类型：
  - 预防性访问控制：试图阻碍或阻止有害的或未授权活动的发生
  - 检测性访问控制：试图发现或检测有害的或未授权的活动
  - 纠正性访问控制：为了发生有害的或未授权的操作，将系统还原至正常状态
  - 威慑性访问控制：为了试图吓阻违反安全策略的活动
  - 恢复性访问控制：为了在出现违反安全策略的情况后修复和还原资源、功能与性能
  - 指令性访问控制：为了指示、限制或者控制主体的活动，从而强制或鼓励主体遵从安全策略
  - 补偿性访问控制：当主控制不能使用或对主控制增加有效性时，补偿性访问控制提供另一种选择
  - 行政管理访问控制：依照组织的安全策略和其他规则或者需求，定义的策略与过程
  - 逻辑/技术性访问控制：作为硬件或软件机制用于提供这些资源或系统的保护
  - 物理性访问控制：控制能物理接触到的东西

13.1.3 CIA三要素

13.2 比较身份标识与认证

- 身份标识是主体声称或自称某个身份的过程
- 通过与有效身份数据库中的一个或多个因素进行对比，身份认证能够认证主体的身份

13.2.1 身份的注册和证明

13.2.2 授权与可问责

- 授权：授权就是指出谁获得信任以执行某具体操作，依据主体的证明身份授予其客体访问权限
- 可问责性：执行审计时用户和其他主体对自己的行为负责，审计、记录和监控都具有可问责性，以此确保主体对自己的行为要负担责任
- 有效的访问控制系统出了满足授权和可问责性外，还需要强大的身份识别和认证机制

12.2.3 认证因素

- 类型1：你知道什么
- 类型2：你拥有什么
- 类型3：你是什么或你做什么

13.2.4 密码

- 最常见的身份认证技术是使用类型1认证方式的密码
- 密码策略
  - 创建强密码
    - 最长使用期
    - 密码复杂度
    - 密码长度
    - 密码历史功能
  - 密码短语：比基本密码更有效的密码机制，列斯与密码字符的字符串
  - 认知密码： 通常是一系列问题，只有主体才知道的实施或预定义答案

13.2.5 智能卡和令牌

智能卡和赢令牌属于身份认证类型2 你拥有什么，一般会和另一种身份认证因素结合使用

1. 智能卡
   - 智能卡是信用卡大小的ID或徽章，中间嵌入了集成地阿奴了芯片，包含了识别或认证的授权信息
2. 令牌
   - 令牌或者赢令牌是一种密码生成设备，用户可以随身携带
   - 硬令牌是一次性动态密码，有两种令牌类型
     - 同步动态密码令牌：基于时间的，并与身份认证服务保持同步
     - 异步动态密码令牌：令牌依据算法和递增计数器生成密码
   - 令牌能提供强大的身份认证，缺点为电池没电和设备中断用户无法访问

13.2.6 生物识别

- 生物识别是属于身份认证类型3 你是什么或你做什么

- 生物识别因素可以用于识别或认证技术，或兼而有之
- 生物识别的方法：
  - 指纹：
  - 脸部扫描：
  - 视网膜扫描：关注眼睛后方血管的图案，最精准的生物识别身份认证形式
  - 虹膜扫描：关注瞳孔周围的有色区域，虹膜扫描通过高品质的图像代替人眼、精度受到灯光变换的影响
  - 手掌扫描：用近红外光测量手掌的经脉模式
  - 手形：是被首部的物理尺寸，轮廓
  - 心跳/脉搏模式：测量用户的脉搏与心跳次数
  - 声音模式识别：依靠一个人说话的声音特点，用户说出一个特定短语，一般是额外验证机制
  - 签字力度：依赖用笔的压力、笔划方式、笔划长度以及提笔时间点
  - 击键模式：分析抬指时间和按压时间来确定主体使用键盘的方式，偏差较大
- 生物识别的错误率：
  - 生物是被最重要的就是准确性，必须检测到信息的微小差异
  - 类型1错误： 错误的身份认证，正确用户的类型1错误率称为错误拒绝率
  - 类型2错误：当无效认证发生时，被成为假正确身份认证，类型2错误率被称为错误接受率
  - 通过较差错误率（CER）：相等错误率
- 生物识别注册：
  - 只有主体被登记或注册，设备才能作为身份标识或身份认证机制使用，被存储的生物识别因素的采样被称为基准轮廓和基准模板

13.2.7 多因素身份认证

- 多因素身份认证时使用两个或多个因素进行认证

13.2.6 设备认证

- 设备指纹：注册期间，设备认证会捕获设备特性

13.3 实施身份管理

- 身份管理技术分两类：集中式和分散式
- 集中式访问控制意味着所有的授权认证都由系统内的单个实体执行
- 分布式访问控制或分散式访问控制意味着授权认证由位于系统中的不同实体执行

13.3.1 单点登录

- 单点登录是一种集中式访问控制技术，允许主体只在系统上认证一次并可以不用认证身份而访问多个资源
- 优点是方便，安全性有增强，缺点是一旦账户被破解，主体就有不受限的访问权限

13.3.2 LDAP和集中式访问控制

- 单个组织经常使用集中式的访问控制系统，目录服务是一个集中式数据库，里面包含了主客体信息。许多目录服务建立在轻量级目录访问协议（LDAP）的基础上。
  - SASL认证：即LDAP提供的在SSL和TLS安全通道基础上进行的身份认证，包括数字证书的认证。
- 访问控制系统经常也会用到多个域和信任关系，安全域是主客体的集合，共用一个安全策略。

13.3.3 LDAP和PKI

- 公钥基础设施（PKI）使用LDAP
- LDAP和集中式访问控制系统可用于支持单点登录功能

13.3.4 Kerberos

- 票据身份认证采用第三方实体证实身份并提供身份身份认证，最知名的票据系统是Kerberos
- Kerberos提供单点登录解决方案以及能够保护登录信息，使用对等秘钥加密AES（秘钥密码），使用端对端的安全机制保障认证通信的机密性和完整性
- 秘钥分发中心（KDC）：提供身份认证服务的可信第三方，所有客户和服务都用KDC注册，秘钥都由KDC维持
- Kerberos身份认证服务器：票据授予服务（KGS）和身份认证服务（AS），身份认证服务认证或拒绝票据的真实性和及时性
- 授予票据：授予票证（TGT）通过KDC提供主体已认证的证明，并授权请求访问其他客体的票据，TGT加密
- 票据：票据是加密的信息，证明主体已被授权访问某个对象
- Kerberos需要账户数据库，它使用客户、网络服务器和KDC之间的票据交换来证明并提供身份认证
- Kerberos的缺点，**存在单点故障，KDC被破解，所有系统的秘钥也都会破解**，KDC离线就无法对主体进行身份认证
- Kerberos也有**严格的时间要求和默认的配置要求**，即所有的系统彼此要在**5分钟**内同步时间。如果本地系统时间超过 5 分钟不同步，有效的TGT 将失效，系统将不会收到任何新票证。

- Kerberos登陆过程如下：
    - 用户将用户名和密码键入客户端
    - 客户端使用AES加密用户名，然后传输至KDC
    - KDC使用已有证书的数据库来认证用户名
    - KDC产生一个同步秘钥，用户客户端和Kerberos服务器间的通信。它加密用户密码的散列值。KDC也生成一个有加密时间戳的授予票证（TGT）.
    - KDC然后传输加密过的同步秘钥和加密过的带有时间戳的TGT客户端
    - 客户端安装TGT，一直使用直至期满。客户端也使用用户的散列解密对称秘钥。
- Kerberos客户端访问资源过程如下：
    - 客户端将其TGT发送回KDC，同时请求访问某个服务器或服务
    - KDC认证TGT有效性并查看其访问控制矩阵，从而认证用户是否拥有能够访问锁请求资源的足够权限
    - KDC生产一个服务票据，然后将它发送至客户端
    - 客户端发送票据至服务器或服务主机
    - 服务器或服务主机通过KDC认证服务票据的有效性
    - 一旦认证了用户身份和授权，Kerberos活动就完成了。服务器或服务主机随后建立与客户端的回话，从而开始进行通信或数据传输

13.3.5 联合身份管理和SSO

- 身份管理是对用户身份和凭证的管理，联合身份管理是多组织加入一个联盟一个组，通过一个方法共享彼此的身份
- 联合身份系统常常使用安全生命标记语言（SAML）或服务配置标记语言（SPML）
    - 超文本标记语言（HTML）：普遍用于展示静态HTML
    - 可扩展标记语言（XML）：超越对数据显示方式，以操控文本的大小和颜色
    - 安全生命标记语言（SAML）：一种基于XML的语言，普遍用于联合组织之间交换认证和授权信息，常为浏览器访问提供单点登录（SSO）功能
    - 服务配置标记语言（SPML）：基于XML的新框架，专门设计用于用户信息交换
    - 访问控制标记语言（XACML）：用于在XML格式内定义访问控制策略，并且通常实现基于角色的访问控制

13.3.6 其他单点登录的例子

- 欧洲安全多环境应用系统（SESAME）：基于邀请的认证系统，开发出来为解决Kerberos的缺点，已不再认为是一款可行的产品
- KryptoKnight：与Kerberos类似，使用对等认证而非第三方，不广泛使用
- OAuth(公开认证):一个开放标准，与HTTP写作，允许用户以单一账户登录
- OpenID:一个开放标准，可与OAuth连同使用，也可单独使用

13.3.7 证书管理系统

- 证书管理系统为用户的凭证保存提供存储空间，证书管理系统确保凭证已加密，从而防止未授权的访问

13.3.8 整合身份服务

- 身份服务未识别和认证提供了额外工具，一些工具是为了基于云的应用程序具体设计的，其他的工具是第三方身份服务，为组织内部使用而设计的
- 身份即服务或者身份和访问即服务（IDaaS）,第三方服务，提供身份和访问管理，为云有效提供单点登录

13.3.9 管理会话

- 无论使用何种认证、重要的是管理会话，以防止未经授权的访问
- 屏幕保护可以配置几分钟时间范围
- 一段时间后安全网络会话也会终止

13.3.10 AAA 协议

- 提供认证、授权和可问责性的协议叫做AAA协议，提供集中式访问控制、并且附带虚拟专用网和其他类型的网络访问服务器的远程控制，保护内部局域网认证系统和其他服务免受远程攻击
- 常见的AAA协议：
  - **RADIUS（远程认证拨号用户服务器）**：主要用于远程连接的身份认证，许多互联网服务提供商（ISP）使用RADIUS进行身份认证，组织也使用RADIUS协议，并与回调安全协议同时执行，实现进一步的保护
    - RADIUS采用用户数据报协议（UDP），并只加密交换密码而不会加密整个会话，也阔以使用附加协议来对数据会话进行加密
  - **TACACS+**：将认证、授权以及可问责性分为独立的流程，可以加密所有的认证信息，使用TCP端口，为数据包提供更高的可靠性
  - **Diameter**：支持多种协议，尤其在支持漫游服务的情况下特别欢迎，使用TCP端口3868或SCTP端口3868，支持IPSec和TLS加密。主要用于移动网络认证如无线设备和智能手机

13.4 管理表示和访问开通生命周期

- 身份信息和访问开通生命周期指账户的创建、管理和删除，开通生命周期的职责:开通、账户审核和账户撤销

13.4.1 开通

- 身份管理的第一步是创建新账号并为其开通相应的权限

13.4.2 账号审核

- 应定期检查账户，以确保正在运行的安全策略

13.4.3 账户撤销

- 无论员工处于何种原因，及时禁用他们的账户十分重要