2 绪论与安全认证

2019年4月10日 22:43

信息安全

- 信息的安全属性
  - 机密性
    - 机密性指对抗对手的被动攻击，保证信息不泄漏给未经授权的实体。
    - 信息的机密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求可以将信息分为不同密级。
  - 完整性
    - 完整性指对抗对手的主动攻击，防止信息被未经授权的篡改。
    - 信息的完整性一方面是指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等；另一方面是指信息处理方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。
  - 可用性
    - 可用性指保证信息及信息系统确实为授权使用者所用。
    - 信息的可用性确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许授权用户或实体可靠而及时地访问信息及资源。
  - 可控性
    - 信息的可控性是指能够控制使用信息资源的人或实体的使用方式。同时，确保信息的所有者可以对信息及信息系统实施安全监控。
  - 抗抵赖性
    - 信息的抗抵赖性也称不可否认性、不可抵赖性，是防止实体否认其已经发生的行为。例如，防止通信双方否认发生过的通信。
    - 信息的不可否认性分为原发不可否认和接受不可否认。原发不可否认用于防止发送者否认自己已发送的数据和数据内容，接受不可否认防止接受者否认已接受的数据和数据内容
- 信息安全的目标
  - 信息安全属性的保持，即通过采用计算机软硬件技术、网络技术、密码技术等安全技术和各种组织管理措施，保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，保持其机密性、完整性、可用性等安全属性
- 信息安全的保护对象
  - 信息安全的概念涵盖了信息、信息载体和信息环境3个方面的安全。信息指信息本身；信息载体指信息的承载体，包括物理平台、系统平台、通信平台、网络平台和应用平台；信息环境指信息及信息载体所处的环境，包括硬环境和软环境

网络安全(Network Security)

- 对于建立在网络基础之上的现代信息系统，网络安全的定义是保护信息系统的硬件、软

件及相关数据，使之不因为偶然或者是恶意的侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。

- 计算机网络，特别是互联网的发展以及网络社会的到来所带来的各类安全问题

网络空间(Cyberspace)

- 网络空间是信息环境中的一个全球域，是和陆、海、空、天相互依存的域之一
- 网络空间由互联互通网络、网络节点和系统及数据组成，可分为物理层、逻辑层和行为体层。
- 通讯系统包括各类互联网、电信网、广电网、物联网、在线社交网络等。

网络空间安全(CyberspaceSecurity)

- 网络空间中所形成的各类安全问题，涉及网络政治、网络经济、网络文化、网络外交、网络军事等诸多领域，形成了综合性和全球性的新特点。
- 较之“网络安全”，网络空间安全更注重空间和全球的范畴。

威胁的来源（CC）

- 环境因素、意外事故或故障：如断电、洪水、火灾、地震等自然灾害，或软件、硬件、通讯线路方面的故障等；
- 无恶意的内部人员：比如内部人员由于缺乏责任心，或缺乏培训，专业技能不足，不具备岗位技能要求而导致信息系统故障或被攻击；
- 恶意的内部人员：不满的或有预谋的内部人员对信息系统进行恶意破坏，或内外勾结盗窃机密信息；
- 第三方：合作伙伴和供应商恶意的和无恶意的行为；
- 外部人员攻击。

脆弱性（漏洞）

- 资产的弱点。脆弱性可能被威胁利用造成安全事件发生，引起资产遭受损害。
- 脆弱性本身无损害，它只是在一定的条件或环境下，为威胁提供了影响资产损失的条件，如果威胁没有发生，脆弱性不会对资产造成损害。

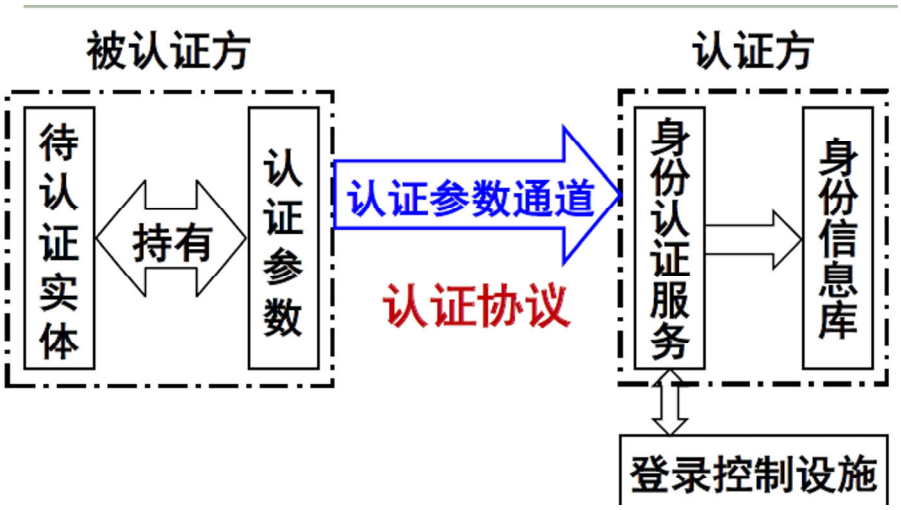
网路空间安全的技术体系

- 设备层安全
    - 应对在网络空间中信息系统设备所面对的安全问题，包括：物理安全，环境安全，设备安全等。
- 系统层安全
    - 应对在网络空间中信息系统自身所面对的安全问题，包括计算机系统安全，网络安全，软件安全等。
- 数据层安全
    - 应对在网络空间中处理数据的同时所带来的安全问题，包括数据安全，身份安全，隐私保护等。

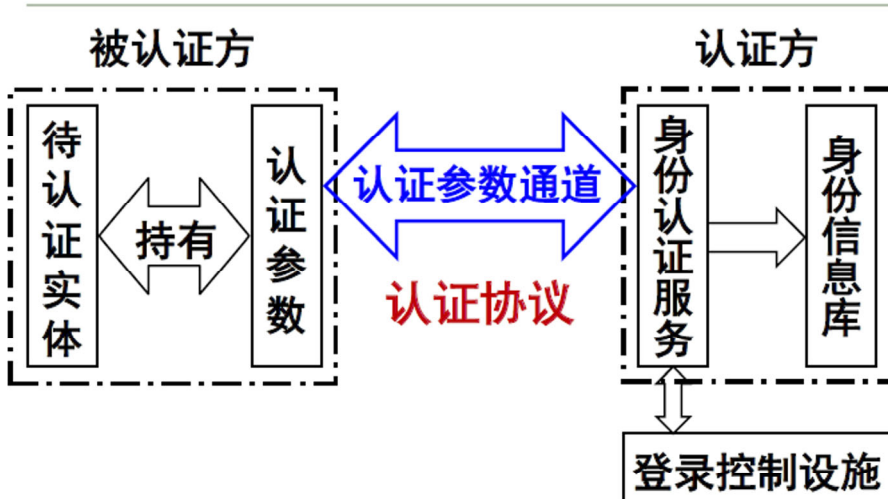
- 应用层安全
  - 应对在信息应用的过程中所形成的安全问题，包括内容安全，应用安全等。

安全认证

1 安全认证概述

- 认证的定义：对实体的身份进行审核，证实其合法性的过程，适用于用户、进程、系统、网络连接等。
- 认证的作用：
  - 识别合法实体与非法实体。
  - 信息系统的第一道安全防线，是访问控制等其它安全机制的基础。
- 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。
- 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或有效。
  - 特点：鉴别过程应该是私密的
- 认证模型(单向)
  - 

- 认证模型(双向)

- 

2 基于知识的身份认证

- 定义：根据用户掌握的知识（What you know）对其进行身份认证。
- 最普遍的技术：基于口令的身份认证。

动态口令技术

- 定义：动态口令(OneTime Password , OTP)，又叫动态令牌、动态密码。
- 基本思想：依据用户身份信息，并引入不确定因子，产生随机变化的口令。

动态口令技术实例：口令序列（S/KEY）

- 初始化
  - 用户产生一个秘密的口令字：SecretPASS（长度大于八个字符）
  - 服务器向用户发送一个种子：SEED（明传）
  - 预处理：MD4(SecretPASS |SEED)，再把16字节的输出结果分为左右2部分，每部分8个字节，这两部分做异或运算，结果记为S。
- 生成口令序列
  - 对S做N次S/KEY安全散列，得到第1个口令；
  - 对S做N-1次S/KEY安全散列，得到第2个口令；
  - 依此类推……
  - 对S做1次S/KEY安全散列，得第N个口令
- 口令的使用
  - 第1个口令发送给服务器端保存
  - 客户端顺序使用第2~N个口令
- 口令的验证
  - 服务器端将收到的一次性口令传给安全hash函数进行一次运算。若与上一次保存的口令匹配，则认证通过并将收到的口令保存供下次验证使用。

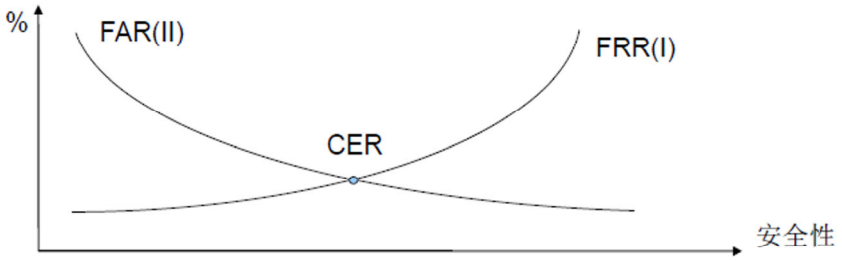
3 基于令牌的身份认证

- 令牌：持有人身份的标志。

    - 特点：唯一、易识别、不易伪造
- 常见的令牌：
    - 智能卡(如银行卡)
        - 利用硬件的不易复制保证用户身份不被仿冒
    - USB Key
        - 智能卡芯片结合USB协议
        - USB接口的、小巧的硬件设备，内置了CPU、存储器、芯片操作系统（COS），可以存储用户的密钥或数字证书，利用USB Key内置的密码算法实现对用户身份的认证。

4 基于生理和行为特征的身份认证

- 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
- 认证系统的误判情况
    - 第一类错误：错误拒绝率(FRR)
    - 第二类错误：错误接受率（FAR）
- 认证系统的准确性
    - 交叉错判率(CER)：FRR=FAR的交叉点，反映系统的准确度。
    -



7 多因素和附加认证技术

- 多因素认证
    - 组合使用两种或两种以上的认证技术，以提高安全性或者可用性。
- 附加认证技术
    - 在基本认证方式（例如用户名+口令）基础上，通过用户的附加信息，例如登录时间、IP地址、MAC地址、地理位置进行认证。
    - 目的：限制用户在特定的时间段、特定主机或地理位置进行访问，提高安全性