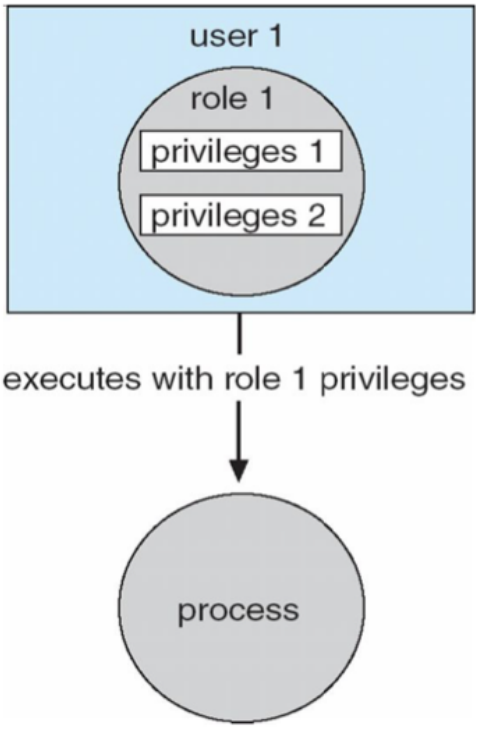
13 Protection & Security in OS

- Protection
  - Goals of Protection
    - 定义
      - Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system.
        - 保护是指控制程序、进程或用户访问计算机系统所定义的资源的一种机制。
    - Goals of Protection:
      - To prevent the access of unauthorized users
        - 防止未授权用户访问
      - To ensure that each active programs or processes in the system uses resources only as the stated policy,
        - 为了确保系统中每个活动的程序或进程只按照规定的策略使用资源，
      - To ensure that errant programs cause the minimal amount of damage possible,
        - 为了确保错误程序造成的损害尽可能小，
      - To improve reliability by detecting latent errors.
        - 通过检测潜在错误来提高可靠性。
  - Principles of Protection
    - Principle of least privilege
      - 最小特权原则
    - ▪ The principle of least privilege dictates that programs, users, and systems be given just enough privileges to perform their tasks.
      - 最小权限原则规定了程序、用户和系统被赋予的权限仅够执行它们的任务。
      - the user account limited privileges
        - 用户帐户限制了权限
      - the root account
        - root帐号
    - ▪ Can be static (during life of system, during life of process)
      - 可以是静态的(在系统寿命期间，在过程寿命期间)
    - ▪ Or dynamic (changed by process as needed) – domain switching, privilege escalation
      - 或动态(根据需要由进程更改)-域切换，特权升级
  - Access Matrix
    - View protection as a matrix (access matrix)

    - 将保护视为矩阵(访问矩阵)
  - Rows represent domains (a domain is a set of object and right pairs)
    - 行表示域(域是一组对象和权限对)
  - Columns represent objects (resources)
    - 列表示对象(资源)
  - Access(i, j) is the set of operations that a process executing in Domain i can invoke on Object j
    - Access(i, j)是在Domain i中执行的进程可以对Object j调用的一组操作
  -

domain \ object	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

- Access Control Policy
  - Role-based access control (RBAC) is a security feature for controlling user access to tasks that would normally be restricted to the root user.
    - 基于角色的访问控制(RBAC)是一种安全特性，用于控制用户对任务的访问，而这些任务通常仅限于根用户。
  - Role-Based Access Control, RBAC, assigns first the roles and then all the permissions are assigned.
    - 基于角色的访问控制(RBAC)首先分配角色，然后分配所有权限。
  - • A user can be assigned multiple roles.
    - •一个用户可以被赋予多个角色。
  - • Multiple users can be assigned the same role.
    - •多个用户可以被赋予相同的角色。
  - • A role can have multiple access rights.
    - •一个角色可以有多个访问权限。
  -

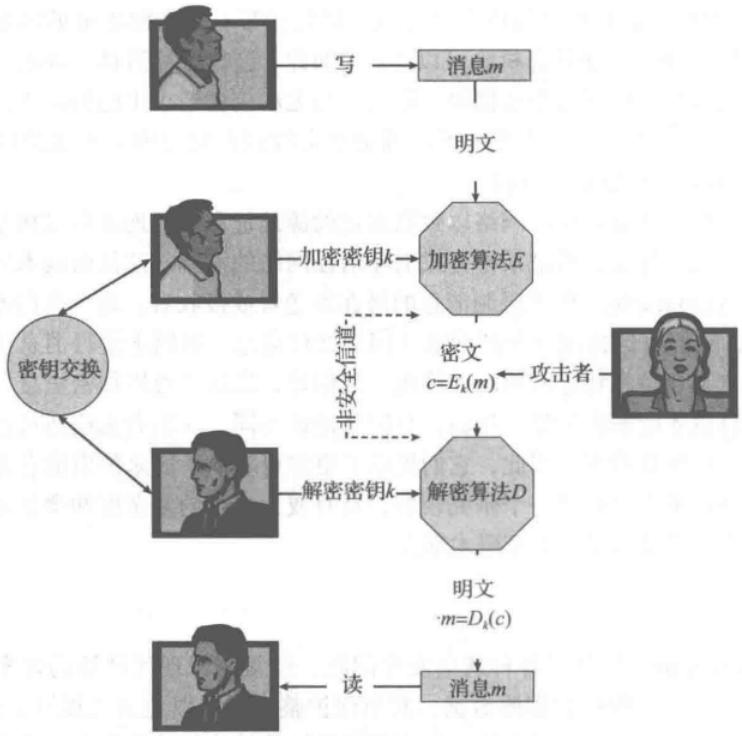


- Security
  - Security Problem
    - Security Violation Categories
      - Breach of confidentiality
        - 违反保密规定
        - Unauthorized reading of data
          - 未经授权读取数据
      - Breach of integrity
        - 违反诚信
        - Unauthorized modification of data
          - 未经授权修改资料
      - Breach of availability
        - 违反可用性
        - Unauthorized destruction of data
          - 未经授权销毁资料
      - Theft of service
        - 盗窃服务
        - Unauthorized use of resources
          - 未经授权使用资源
      - Denial of service (DOS)
        - 拒绝服务(DOS)
        - Prevention of illegitimate use

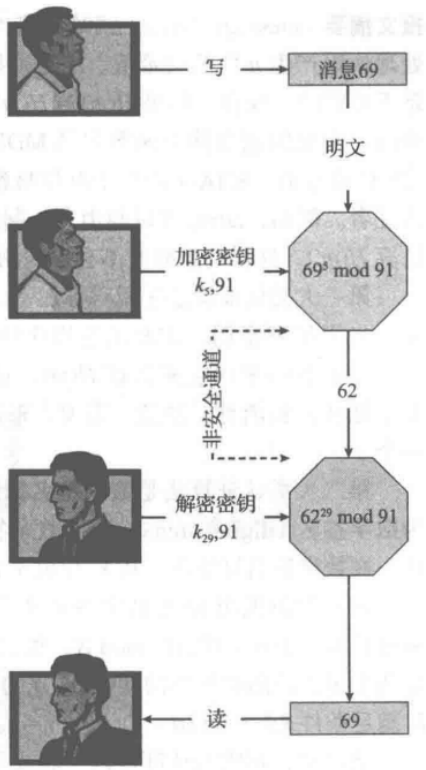
        - 防止非法使用
- The Security Problem
    - Concepts used in security
        - Intruders (crackers) attempt to breach security
            - 入侵者(骇客)试图破坏安全性
        - Threat is potential security violation
            - 威胁是潜在的安全违规
        - Attack attempts to breach security
            - 攻击试图破坏安全性
            - Attack can be accidental or malicious
                - 攻击可以是偶然的，也可以是恶意的
            - Easier to protect against accidental than malicious misuse
                - 更容易防止意外而不是恶意误用
- Security Violation Methods
    - Masquerading (breach authentication)
        - 伪装(违规认证)
        - attacker pretends to be an authorized user to escalate privileges
            - 攻击者冒充授权用户升级权限
    - Replay attack
        - 重放攻击
        - attacker delays, replays, or repeats data transmission between the user and the site.
            - 攻击者延迟、重放或重复用户与站点之间的数据传输
            - 微信两次一样的付款
    - Man-in-the-middle attack
        - 中间人攻击
        - intruder sits in data flow, masquerading as sender to receiver and vice versa
            - 入侵者位于数据流中，伪装成发送方到接收方，反之亦然
    - Hijacking
        - 劫持
        - type of network security attack in which the attacker takes control of computer systems, software programs etc.
            - 一种网络安全攻击，攻击者控制计算机系统、软件程序等。
- Program Threats
    - Trojan Horse - allows programs written by users to be executedby other users (Spyware, pop-up browser windows, covert channels)

        - 特洛伊木马-允许用户编写的程序由其他用户执行(间谍软件，弹出式浏览器窗口，隐蔽通道)
    - Trap Door - is when a hacker deliberately inserts a security hole that they can use later to access the system.
        - 陷阱门-是指黑客故意插入一个安全漏洞，他们可以使用以后访问系统。
    - Logic Bomb - is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
        - 逻辑炸弹——是故意插入软件系统的一段代码，当满足特定条件时，它将触发恶意功能。
    - Stack and Buffer Overflow exploits a bug in a program (overflow either the stack or heap buffers)
        - 堆栈和缓冲区溢出利用程序中的错误(溢出堆栈或堆缓冲区)
    - Viruses - fragment of code embedded in an otherwise legitimate program, designed to replicate itself (by infecting other programs), and (eventually) wreaking havoc.
        - 病毒——嵌入在合法程序中的代码片段，旨在自我复制(通过感染其他程序)，并(最终)造成严重破坏。
- System and Network Threats
    - Worm - is a process that uses the fork process to make copies of itself in order to create chaos in a system. Worms consume system resources, often blocking out other, legitimate processes.
        - 蠕虫-是一个进程，它使用分叉进程来复制自己，以便在系统中制造混乱。蠕虫消耗系统资源，经常阻塞其他合法进程。
    - Port Scanning is technically not an attack, but rather a search for vulnerabilities to attack.
        - 端口扫描在技术上不是攻击，而是搜索可攻击的漏洞。
    - Denial of Service (DOS) attacks that attempt to lock down systems so much that they can no longer be used for any useful activity. DOS attacks can also involve social engineering.
        - 拒绝服务(DOS)攻击，试图锁定系统，使其不能再用于任何有用的活动。DOS攻击还可能涉及社会工程。
- Security Measure Levels
    - To protect a system, we must take security measures at four levels:
    - Physical
        - Data centers, servers, connected terminals
            - 数据中心，服务器，连接终端
    - Human
        - Avoid social engineering, phishing (involves sending an innocent-looking e-mail), dumpster diving (searching the trash or other locations for

passwords),password cracking.
    - 避免社会工程、网络钓鱼(包括发送看似无辜的电子邮件)、垃圾箱搜索(在垃圾桶或其他地方搜索密码)、密码破解。
  - Operating System
    - System must protect itself from accidental or purposeful security breaches:runaway processes (DOS denial of service), memory-access violations ,stack overflow violations, the launching of programs with excessive privileges, etc.
      - 系统必须保护自己免受意外或有目的的安全破坏:失控进程(DOS拒绝服务)，内存访问违规，堆栈溢出违规，启动具有过多特权的程序等。
  - Network
    - protecting the network itself from attack and protecting the local system from attacks coming in through the network (intercepted communications, interruption, DOS, etc).
      - 保护网络本身不受攻击，保护本地系统不受来自网络的攻击(通信截获、中断、DOS等)。
- Cryptography as a Security Tool
  - Encryption
    - Cryptography is a technique to hide the message using encryption.
      - 密码学是一种使用加密来隐藏消息的技术
    - Encryption is a process of encoding a message so that its meaning can not be easily understood by unauthorized people.
      - 加密是对信息进行编码的过程，使其含义不能被未经授权的人轻易理解
  - Symmetric Encryption对称加密
    - Same key used to encrypt and decrypt
      - 用于加密和解密的密钥相同
    - Data Encryption Standard (DES) was most commonly used symmetric block-encryption algorithm (created by US Govt)
      - 数据加密标准(DES)是最常用的对称块加密算法(由美国政府创建)
    - Triple-DES considered more secure
      - 三重des被认为更安全
    - Advanced Encryption Standard (AES)
      - 高级加密标准(AES)
    - Rivest Cipher RC4 is most common symmetric stream cipher, but known to have vulnerabilities
      - Rivest Cipher RC4是最常见的对称流密码，但已知存在漏洞



- Asymmetric Encryption非对称加密
  - 比特币
  - Public-key encryption based on each user having two keys
    - 基于每个用户拥有两个密钥的公钥加密
    - public key – published key used to encrypt data
      - 公钥-用于加密数据的已发布密钥
    - private key – key known only to individual user used to decrypt data
      - 私钥-仅为用于解密数据的单个用户所知的密钥
  - Most common is RSA (RSA = Ron Rivest, Adi Shamir and Leonard Adleman)based on prime numbers
    - 最常见的是基于质数的RSA (RSA = Ron Rivest, Adi Shamir和Leonard Adleman)

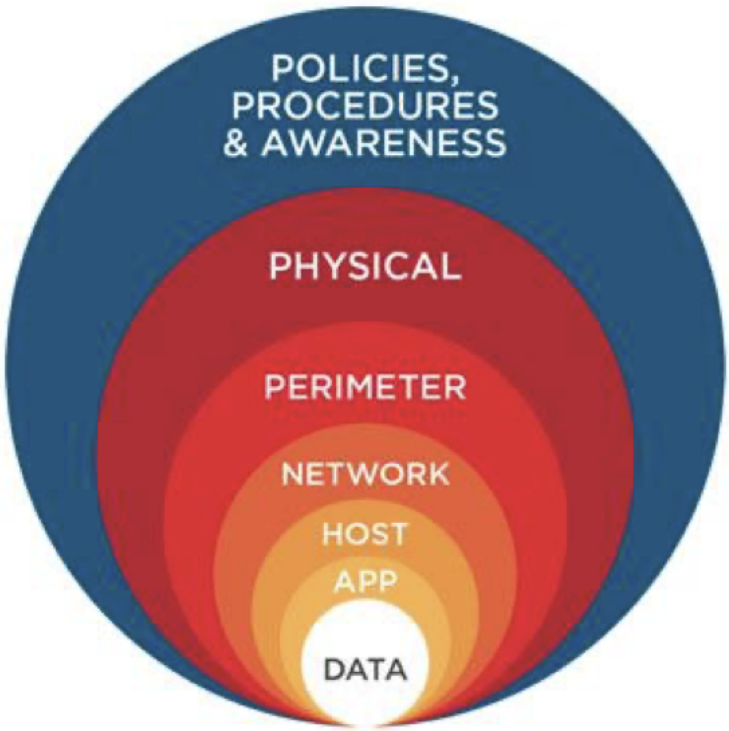


- Authentication Digital Certificates
  - Is the public key safe?
    - 公钥安全吗?
  - One solution : digital certificates
    - 一个解决方案:数字证书
  - A digital certificate is a mechanism that allows users to verify the authenticity of a key / document.
    - 数字证书是一种允许用户验证密钥/文档真实性的机制。
    - Proof of who or what owns a public key
      - 谁或什么拥有公钥的证明
    - Public key digitally signed a trusted party
      - 公钥数字签名的可信方
    - Trusted party receives proof of identification from entity and certifies that public key belongs to entity
      - 受信任方从实体接收身份证明，并证明公钥属于实体
    - Certificate authority are trusted party – their public keys included with web browser distributions
      - 证书颁发机构是受信任的一方——它们的公钥包含在web浏览器发行版中
      - They vouch for other authorities via digitally signing their keys
        - 他们通过对密钥进行数字签名来为其他权威机构担保
- Key Distribution Management

        - Keys in Symmetric encryption is a major problem
            - 对称加密中的密钥是一个主要问题
        - One option is to send them Out-of-band, say via paper or a confidential conversation or One-time pad
            - 一种选择是将它们发送到带外，例如通过纸张或机密谈话或一次性记事本发送
        - Keys in Asymmetric encryption - the public keys are not confidential.
            - 非对称加密中的密钥——公钥不是机密的。
            - the key-ring can be easily stored and managed (key-ring is simply a file with keys in it.).
                - key-ring可以很容易地存储和管理(key-ring只是一个包含密钥的文件)。
        - Even asymmetric key distribution needs care – man-in-the-middle attack
            - 即使是非对称密钥分发也需要小心——中间人攻击
- User Authentication
    - Authentication
    - When a user logs into a computer, the OS needs to determine the identity of the user.
        - 当用户登录计算机时，操作系统需要确定用户的身份。
    - The user authentication has two steps:
        - 用户身份验证分为两个步骤:
        - Identification - a unique identifier is specified to the user to authenticate.
            - 识别——为用户指定一个唯一的标识符进行认证。
            - • a Signing function - produces an authenticator: a value to be used to authenticate a user.
                - 一个签名函数——生成一个认证器:一个用于认证用户的值。
        - Verification of a user - performed against the unique identifier ,that is, it confirms the binding between the user and the identifier.
            - 对用户的验证——对唯一标识符进行验证，即确认用户与标识符之间的*绑定关系*。
            - a Verification function - produces a value of "true" if the authenticator was created from the user, and "false" otherwise.
                - -验证函数——如果验证者是由用户创建的，则生成值为“true”，否则生成值为“false”。
    - two main authentication algorithms :
        - 1. Message Authentication Code (MAC): uses symmetric encryption.
            - 1. MAC (Message Authentication Code):采用对称加密。

- • a cryptographic checksum is generated from the message using a secret key.
  - •使用密钥从消息生成加密校验和。
- 2. Digital-signature algorithm - uses asymmetric encryption.
  - 2. 数字签名算法——使用非对称加密。
  - A person can encrypt signature related data with the use of a private key
    - 一个人可以使用私钥加密签名相关的数据
  - One can give the public key to anyone who needs verification of the signer's signature.
    - 你可以将公钥提供给任何需要验证签名者签名的人
- Common forms of user authentication
  - Passwords
    - Password Vulnerabilities
      - 密码漏洞
    - Securing Passwords - modern systems do not store passwords in clear-text form.
      - 保护密码——现代系统不以明文形式存储密码。 *********
    - One-time passwords resist shoulder surfing and other attacks .
      - 一次性密码可以抵御肩头冲浪和其他攻击。
  - Biometrics involve a physical characteristic of the user.
    - 生物识别技术涉及用户的身体特征。
  - Multifactor authentication is better.
    - 多因素身份验证更好
- Implementing Security Defenses
  - The major methods, tools, and techniques that can be used to improve security:
    - 可用于提高安全性的主要方法、工具和技术:
    - Security Policy
      - 安全策略
    - Vulnerability Assessment
      - 漏洞评估
    - Intrusion Detection
      - 入侵检测
    - Virus Protection
      - 病毒防护
    - Auditing, Accounting, and Logging
      - 审计、会计和日志

- Defense in depth is most common security theory – multiple layers of security
  - 深度防御是最常见的安全理论——多层安全



- Vulnerability Assessment
  - How can we determine whether a security policy has been correctlyimplemented?
    - 我们如何确定安全策略是否已被正确实现?
  - Periodically examine the system to detect vulnerabilities.
    - 定期检查系统，及时发现系统漏洞。
    - ❑ Port scanning.
      - 端口扫描。
    - ❑ Check for bad passwords.
      - 检查不良密码。
    - ❑ Unauthorized programs in system directories.
      - 系统目录中未经授权的程序。
    - ❑ Incorrect permission bits set.
      - 设置的权限位不正确。
    - ❑ Program checksums / digital signatures which have changed.
      - 改变了的程序校验和/数字签名
    - ❑ Unexpected or hidden network daemons.
      - 意外的或隐藏的网络守护进程。
    - ❑ New entries in startup scripts, shutdown scripts or other system scriptsor configuration files.

        - 启动脚本、关闭脚本或其他系统脚本或配置文件中的新条目。
    - ❑ New unauthorized accounts.
        - 新的未经授权的帐户。