任务一：标准研读

1. 请解释引用监控器和可信计算基的基本概念，并阅读国标 GB17859-1999 和对应的美国 TCSEC 标准，区分 GB17859-1999 第三级与第四级安全要求的异同之处、以及第四级与第五级安全功能要求的异同之处？

2、请阐述 CC 标准中的脆弱性(vulnerability)、威胁(threat)和风险(risk) 概念及其相关关系，并参考 CC 标准文档和鸿蒙系统 ST 安全目标文档（自己到 CC 官网下载），以鸿蒙系统 ST 为例，说明 CC 对 ST 文档的规范格式，并说明鸿蒙系统主要考虑了那些安全威胁，实现了那些安全功能，提供了那些安全保证技术？

1.1 引用监控器和可信计算基的基本概念

- **引用监控器（Reference Monitor）**：监控主体和客体之间授权访问的部件。

- **可信计算基（trusted computing base）**：计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

1.2 GB17859-1999 第三级与第四级安全要求的异同之处

（1）第四级要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。

- 第三级：计算机信息系统可信计算基应维护与主体及其控制的存储客体（例如：进程、文件、段、设备）相关的敏感标记。（4.3.3 标记）
- 第四级：计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统资源（例如：主体、存储客体、只读存储器）相关的敏感标记。（4.4.3 标记）

（2）第四级还要考虑隐蔽通道。

第四级：计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。（4.5.6 审计）系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。（4.4.8 隐蔽信道分析）

（3）第四级加强了鉴别机制。

第四级：对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。（4.4.9 可信路径）

除此之外要求均相同。

1.3 GB17859-1999 第四级与第五级安全功能要求的异同之处

（1）第五级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。

访问控制能够为每个命名客体指定命名用户和用户组，并规定他们对客体的访问模式。（4.5.1 自主访问控制）

（2）第五级支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号。

计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们。（4.5.6 审计）

（3）第五级对可信路径做了进一步要求。

对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。（4.4.9 可信路径）

当连接用户时（如注册、更改主体安全级），计算机信息系统可信计算基提供它与用户之间的可信通信路径。可信路径上的通信只能由该用户或计算机信息系统可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分。（4.5.9 可信路径）

（4）第五级提供系统恢复机制。

计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。（4.5.10）

除此之外要求均相同。

2.1 CC 标准中的脆弱性(vulnerability)、威胁(threat)和风险(risk) 概念及其相关关系。

相关概念：

(1) **脆弱性**：在一些情况下，TOE 中可能被用于违反安全功能需求的弱点/缺陷。

示例：数据库存在未修复的 Bug，可能使攻击者获得系统权限

原文定义：

vulnerability ：weakness in the target of evaluation (TOE)(3.90) that can be used to violate the security functional requirements (SFRs) (3.78) in some environment.

potential vulnerability：suspected, but not confirmed, weakness.（疑似但未被确认的弱点。）

residual vulnerability：weakness that cannot be exploited in the operational environment (3.63) for the target of evaluation (TOE)(3.90), but that can be used to violate the security functional requirements (SFRs) (3.78) by an attacker with greater attack potential (3.8) than is anticipated in the operational environment for the TOE

（2）威胁：可能利用脆弱性对系统或资产造成不期望影响的潜在因素。

示例：黑客攻击有 Bug 的数据库（人为因素）；洪水火灾（自然因素）

（3）风险：威胁利用脆弱性，导致系统或资产受损、破坏的潜在可能。

示例: 如果一个企业的数据库存在脆弱性，而该企业知道有黑客组织在寻找这类脆弱性，那么该企业面临的风险就是这个数据库被攻破，导致数据泄露的可能性。

（二）关系：

风险通常基于威胁和脆弱性的相对存在来量化。当系统存在脆弱性并且有威胁可能利用这些脆弱性时，系统才面临风险。如果其中一个因子不存在，那么风险就是零。其可以简单用一个公式来进行描述这种关系：

$$\text{风险} = \text{脆弱性} \times \text{威胁}$$

例如，即使一个系统存在脆弱性，但如果没有威胁来利用它，系统面临的风险就很低。相反，如果系统没有脆弱性，即使面临很多威胁，它的风险也很低。

从安全的系统角度来看：

资产的脆弱性可能会被威胁者利用，从而造成资产的风险，这个过程也可以理解为威胁会增加潜在的风险，从而对最终的资产造成威胁。资产所有者应分析可能的威胁并确定哪些存在于他们的环境，其结果就是风险。这种分析会有助于对策的选择，以应对风险并将其降低到一个可接受的水平。

脆弱性、威胁和风险之间的关系如图所示。

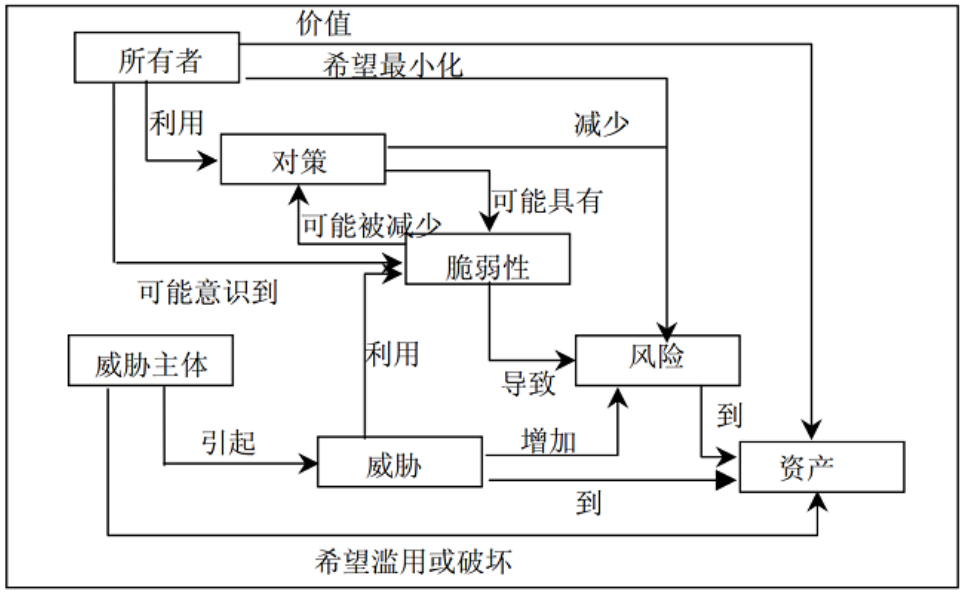

图 2-1 脆弱性、威胁和风险之间的关系

2.2 对于鸿蒙系统的 Security Target 文档，它遵循了 CC 标准中规定的组织结构和内容，包括但不限于：

(1) **引言（Introduction）**：介绍 Security Target 文档的目的和范围，以及鸿蒙系统的背景和概述。

(2) **规范性引用**：列举了与 Security Target 文档相关的标准和文献的引用。

(3) **安全目标**：明确了鸿蒙系统的安全目标，包括对不同安全领域的要求。

(4) **安全功能**：详细描述了鸿蒙系统实现的安全功能，包括访问控制、信息流控制、安全审计等。

(5) **安全保证**：提供了鸿蒙系统的安全保证技术和机制，如漏洞管理、代码审查、密钥管理等。

(6) **安全需求确认**：明确了对鸿蒙系统的安全评估的要求和方法。

(7) **安全目标合理性论证**：解释了鸿蒙系统的安全目标确定的理由和基础。

2.3 鸿蒙系统主要考虑了以下安全威胁：

(1) **未经授权访问**：鸿蒙系统的安全目标包括提供严格的访问控制机制，确

保只有经过授权的用户可以访问系统资源和数据。

(2) **数据泄露：**鸿蒙系统致力于保护用户的敏感数据不被泄露。它采用了各种加密技术，包括对存储的数据进行加密、传输数据的安全通信、以及对用户识别和认证信息的保护，以确保数据的机密性和完整性。

(3) **恶意软件和攻击：**鸿蒙系统具有强大的安全功能，包括恶意软件扫描和检测机制、安全隔离和权限管理，以及针对漏洞和攻击的快速修复和更新机制。它还采用了安全更新和固件验证技术，确保系统始终保持在最新的安全状态。

(4) **用户隐私保护：**鸿蒙系统关注用户的隐私保护。它提供了强大的用户身份认证和权限管理机制，确保用户的个人信息和隐私得到保护。此外，系统采用了隐私数据保护措施，限制应用程序对用户敏感数据的访问和使用。

(5) **物理攻击和非法访问：**鸿蒙系统提供了针对物理攻击和非法访问的安全保护措施。它具有安全启动机制和安全启动检测，以确保系统在启动过程中不受恶意修改或篡改。系统还采用了硬件安全技术，如可信执行环境（TEE）、安全元（SE）、防篡改芯片等，以提供额外的安全保护。

2.4 以下是鸿蒙系统的主要安全功能和安全保证技术的详细说明：

(1) **访问控制：**鸿蒙系统采用访问控制机制来保护系统资源和用户数据的访问。该系统实现了基于权限的访问控制，使用权限来限制用户和系统进程对资源的访问。

(2) **安全认证和身份验证：**鸿蒙系统提供了安全的用户认证和身份验证功能。用户在进行敏感操作之前必须通过有效的身份验证才能访问系统资源。

(3) **加密和数据保护：**鸿蒙系统支持数据的加密和保护，确保用户数据的机密性和完整性。它提供了安全的数据传输和存储功能，包括加密文件系统、加密通信等。

(4) **安全传输层：**鸿蒙系统提供了安全传输层，用于保护敏感数据在网络上的传输。该传输层使用安全协议和加密算法来防止数据的窃听和篡改。

(5) **安全漏洞修补：**鸿蒙系统定期发布安全补丁，修补已知的安全漏洞，以

保护系统免受已知的安全威胁。

(6) **安全审计和监控：**鸿蒙系统具有安全审计和监控功能，用于监视系统的安全操作和行为。它记录关键操作和事件，帮助鉴定潜在的安全问题。

(7) **可信执行环境：**鸿蒙系统提供了可信的执行环境，用于运行敏感应用程序。这个环境提供了硬件级别的安全保护，防止恶意软件和攻击者对系统的入侵。

(8) **安全更新和远程管理：**鸿蒙系统支持安全的远程管理和更新功能，以保持系统的安全性。它提供了安全的远程访问机制，确保固件和软件的安全升级。