**第二次作业**

**作业要求：**

1. **按小组完成，提交作业文档和PPT。**
2. **每组选择两个任务之一完成。**
3. **对于每个选题，被选中的小组（助教10月22日24时前通知）要求课堂上陈述（请每个小组提前安排好陈述同学），而且每个组至少准备和现场提2个问题（针对其他组的陈述进行提问，否则将影响评分等级）。**
4. **提交文档和PPT时间为10月22日22时，提交给张鑫汇总后发给老师。**

请每个小组完成以下两个任务：

**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？**

**任务二：Linux IMA机制分析**

**1．在了解TPM安全芯片的组成和作用基础之上，基于计算平台信任链扩展技术，分析Linux内核的IMA模块实现的信任链由OS层扩展到用户应用层的功能，主要完成：**

**1）编写以下示例代码，通过加载或运行，观察Linux IMA是如何发生作用的。**

**（1）用户应用程序**

**（2）共享库**

**（3）内核模块**

**2）对Linux IMA的实现源代码进行分析，重点解析：**

**（1）IMA模块中与度量值表示和存储相关的数据结构**

**（2）IMA模块中与度量对象识别相关的分析代码**

**（3）IMA模块中与度量值计算相关的算法**

**（4）与IMA模块自身安全保护相关的机制和代码（如EVM机制）**