作业五

(密码学与网络安全课程报告)

姓　　名：肖文韬

学　　号：2020214245

专 业 方 向：电子信息（计算机技术）

邮　　箱：xwt20@mails.tsinghua.edu.cn

二〇二一年五月四日

第 1 章　作业内容

1. 简述可信计算机系统评估准则 (TCSEC)。

   答：

   可信计算机系统评估准则是信息安全技术的里程碑，1985 年作为美国国防部标准（DoD）发布（DoD 5200.28-STD）。主要为军用标准，延用为民用。主要针对主机型分时操作系统，主要关注保密性。安全级别主要按功能分类，安全级别从高到低分别为 A、B、C、D 四级，级下再分小级，包含 D、C1、C2、B1、B2、B3、A1 这七个级别。后发展为彩虹系列。

   (a) (无保护)D 级：该级的计算机系统除了物理上的安全设施外没有任何安全措施，任何人只要启动系统就可以访问系统的资源和数据，如 DOS, Windows 的低版本和 DBASE 均是这一类 (指不符合安全要求的系统, 不能在多用户环境中处理敏感信息)。

   (b) (自主保护类)C1 级：具有自主访问控制机制、用户登录时需要进行身份鉴别。

   (c) (自主保护类)C2 级：具有审计和验证机制 ((对 TCB) 可信计算机基进行建立和维护操作，防止外部人员修改)。如多用户的 UNIX 和 ORACLE 等系统大多具有 C 类的安全设施。

   (d) (强制安全保护)B1 级：引入强制访问控制机制，能够对主体和客体的安全标记进行管理。

   (e) (强制安全保护)B2 级：具有形式化的安全模型，着重强调实际评价的手段，能够对隐通道进行限制。(主要是对存储隐通道)

   (f) (强制安全保护)B3 级：具有硬件支持的安全域分离措施，从而保证安全域中软件和硬件的完整性，提供可信通道。对时间隐通道的限制。

   (g) (验证保护)A1 级：要求对安全模型作形式化的证明，对隐通道作形式化的分析，有可靠的发行安装过程。

   彩虹系列：

   (a) 桔皮书：可信计算机系统评估准则

   (b) 黄皮书：桔皮书的应用指南

   (c) 红皮书：可信网络解释

   (d) 紫皮书：可信数据库解释

TCSEC 缺陷：

(a) 集中考虑数据保密性，而忽略了数据完整性、系统可用性等；

(b) 将安全功能和安全保证混在一起；

(c) 安全功能规定得过为严格，不便于实际开发和测评。

2. 简述计算机信息系统安全保护等级划分准则。

答：

《中华人民共和国计算机信息系统安全保护条例》第九条明确规定，计算机信息系统实行安全等级保护。公安部组织制订了《计算机信息系统安全保护等级划分准则》国家标准（GB/T 17859），于 1999 年 9 月 13 日由国家质量技术监督局审查通过并正式批准发布，于 2001 年 1 月 1 日执行。该准则的发布为计算机信息系统安全法规和配套标准的制定和执法部门的监督检查提供了依据，为安全产品的研制提供了技术支持，为安全系统的建设和管理提供了技术指导是我国计算机信息系统安全保护等级工作的基础。

中国已经发布实施的《计算机信息系统安全保护等级划分准则》GB17859-1999。这是一部强制性国家标准，也是一种技术法规。它是在参考了 DoD 5200.28-STD 和 NCSC-TC-005 的基础上，从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径和可恢复等 10 个方面将计算机信息系统安全保护等级划分为 5 个级别的安全保护能力。

(a) 用户自主保护级：本级的计算机信息系统可信计算机通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

(b) 系统审计保护级：与用户自主保护级相比，本级的计算机信息系统可信计算机实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

(c) 安全标记保护级：本级的计算机信息系统可信计算机具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

(d) 结构化保护级：本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它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。此外，还要考虑隐蔽通道。

(e) 访问验证保护级：本级的计算机信息系统可信计算机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。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。

3. 什么是可信计算基？详细说明安全标记保护级的可信计算基的功能。

答：

可信计算基的定义：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。它建立了一个基体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。一旦可信计算机基的某个构件出现程序错误或者安全隐患，就对整个系统的安全造成危害。与之相反，如果除可信计算基之外的系统的其他部分出现问题，也只是泄漏了系统安全策略赋予它们的相关权限而已，这些权限一般都是比较低的。

安全标记保护级的可信计算基的功能有：

(a) 自主访问控制：计算机信息系统可信计算基定义和控制系统中命名用户对命名客体地访问。

(b) 强制访问控制：计算机信息系统可信计算基对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。

(c) 标记：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。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

(d) 身份鉴别：计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算基使用这些数据鉴别用户身份，并使用保护机制（例如：口令）来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。

(e) 客体重用：在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤消客体所含信息的所有授权。

(f) 审计：计算机信息系统可心计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

(g) 数据完整性：计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权拥护修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4. 收集有关信息安全的定义、标准等方面的最新概念和进展。

答：

信息安全标准是确保信息安全的产品和系统在设计、研发、生产、建设、使用、测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。信息安全标准是我国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要手段。信息安全保障体系的建设、应用，是一个极其庞大的复杂系统，没有配套的安全标准，就不能构造出一个可用的信息安全保障体系。

国际上，信息安全标准化工作，兴起于二十世纪 70 年代中期，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注目前。目前世界上约有近 300 个国际和区域性组织，制定标准或技术规则，与信息安全标准化有关的主要的组织有：国际标准化组织 (ISO)、国际电工委员会（IEC）、国际电信联盟（ITU）、Internet 工程任务组（IETF）等。

目前，我国按照国务院授权，在国家质量监督捡验捡疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，下设有 255 个专业技术委员会。中国标准化工作实行统一管理与分工负责相结合的管理体制，有 88 个国务院有关行政主管部门和国务院授权的有关行业协会分工管理本部门、本行业的标准化工作，有 31 个省、自治区、直辖市政府有关行政主管部门分工管理本行政区域内本部门、本行业的标准化工作。成立于 1984 年的全国信息技术安全标准化技术委员会（CITS），在国家标准化管理委员会和信息产业部的共同领导下负责全国信息技术领域以及与 ISO/IEC JTC1 相对应的标准化工作，目前下设 24 个分技术委员会和特别工作组，是目前国内最大的标准化技术委员会。它是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。全国信息技术安全标准化技术委员会的工作范围是负责信息和通信安全的通用框架、方法、技术和机制的标准化，归口国内外对应的标准化工作。其技术安全包括：开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。

目前 TC26059 已发布了安全标准 140 余项，CCSA 发布或起草的通信领域安全标准共计 230 多个，涉及信息安全技术与机制、信息安全管理、信息安全评估以及保密、密码和通信安全等领域。以 2014 年 ITU-T SG17 会议为例，在全部 63 篇提案文稿中，我国占 23 篇，最终被采纳 19 篇。2013 年我国主导研制的云计算安全标准《云计算安全框架》获批成为国际标准，2015 年智能制造总体标准《工业物联网背景下的智能制造概述》在 ITU-T 立项，我国在国际安全标准领域的话语权逐步提升。

5. 简述侧信道攻击的原理、分类和对策。

答：

侧信道密码分析（Side Channel Attack）利用密码系统实现时泄露的额外信息，推导密码系统中的秘密参数。包括计算错误、执行时间、能量消耗、电磁辐射。

攻击与具体的实现有关，因此不是通用的，但比古典密码分析更强大，能够在极少的时间内攻破密码系统，被认为是对密码实现设备的严重威胁美国评估 AES 过程中，密码学界就打成共识：即使密码算法对传统密码分析是安全的，但如果不能安全的实现，该算法也是无用的。

侧信道攻击可以分为入侵型、非入侵型和半入侵型攻击：

(a) 入侵型攻击：通过特殊工具对设备进行物理篡改。需打开卡片直接访问芯片表面，如揭开智能卡保护层，直接在数据总线上连线，观察数据传输。可不干扰芯片正常操作

(b) 非入侵型攻击：只利用暴露在外部的可用信息，如运行时间、能量消耗等

(c) 半入侵型攻击：也需要打开卡片，访问芯片表面，但不去篡改钝化层，也就是对金属表面不需要电接触

侧信道攻击还可以分为主动攻击和被动攻击：

(a) 主动攻击：是指攻击者篡改芯片的正常操作功能，例如在芯片计算过程中引入错误，发起错误攻击

(b) 被动攻击：只是观察芯片处理数据的行为，收集可利用的侧信道信息，而不去干扰芯片的操作。被动攻击也可能是入侵型攻击，因为可能需要打开芯片，以便于更好地收集信息

错误攻击的对策：

密码设备首先验证操作的结果，只有当结果正确的时候才输出结果。验证需

要额外的操作，势必损失效率。DES 加密，可以对明文加密两次，如果两次加密结果相同便认为加密过程没有出现错误，也可以使用解密操作验证 DES 密文正确性。随机化操作也可以抵抗错误攻击。对于 RSA 算法，首先对信息使用随机位填充，然后再进行加密或签名。智能卡可以采用入侵检测和自检测对付错误引入。

时间攻击的对策：

(a) 隐藏时间差别，比如增加随机延迟

(b) 隐藏内部状态

能量攻击的对策：

消除与秘密参数相关的条件分支。如果能量消耗与操作数相关，可以使用秘密共享中的门限方案，把操作数分解成多个“影子”并分别处理，在这种情况下，可使用高阶 DPA 进行攻击，但多个“影子”有效地增加了噪音，从而增加攻击难度；也降低了系统的性能。插入随机计算是一种对付 DPA 的通用方法。例如在执行加密时，随机地插入虚假运算，从而每次加密都产生不同的能量迹，加大 DPA 的难度。将硬件组件（如电容）增加到智能卡的能源线上，使外部电源不直接连接内部芯片，从而降低能量消耗与内部操作的相关性，以此过滤、平滑能量消耗特征，减低能量消耗偏差，增加 DPA 攻击所需的能量迹。

6. 简述数字水印的特点。

答：

数字水印技术属于信息隐藏技术的一个分支。

特点和要求：

(a) 水印要直接嵌入数据中：而不是将水印放在数据文件的头部或尾部等位置。

(b) 透明性：不影响原数据的使用价值，如：不影响图像的视觉效果、真实性，不容易被人的知觉系统觉察，或不易引起人的注意。

(c) 鲁棒性：不同的应用对鲁棒性要求不一样，一般都应能抵抗正常的图像处理，例如滤波、直方图均衡等。用于版权保护的鲁棒水印需要最强的鲁棒性，需要抵抗恶意攻击，而易损水印、注释水印不需抵抗恶意攻击。

(d) 安全性：一个水印体制要走向商业应用，其算法必须公开。算法的安全性完全取决于密钥，而不是对算法进行保密以取得安全性。所以，密钥空间需足够大，而且分布比较均匀。另外，鲁棒水印需要能抵抗各种恶

意攻击，易损水印要能抵抗“伪鉴别”攻击。