主题4作业

**小组成员：**

王世泽 - S202175111

杨悦 - S202175112

张思远 - S202175103

肖杏梅 - S202175098

呼佳嘉 - S202175019

**创建日期:** 2021-10-18

**更新日期:** 2021-10-18

**当前版本：**1.2

# 文档控制

## 变更记录：

|  |  |  |  |
| --- | --- | --- | --- |
| 变更日期 | 版本号 | 变更人 | 变更内容 |
| 2021-10-18 | V1.1 | 肖杏梅 | 创建文本、编写内容 |
| 2021-10-19 | V1.2 | 呼佳嘉 | 完善文本内容，整理结构 |
|  |  |  |  |
|  |  |  |  |

# 相关内容

**1.概述（什么是可信计算、可信性、国内外研究现状）**

**可信计算：**

可信计算技术是一种由可信计算组开发并推出的技术。可信的意义在于确保软件或者系统运行期间的完整性，以此保证软件或系统最终的运行状态符合最初的预期设计目标，从而使系统或软件的运行处于可信的环境中。可信是安全的前提条件，保证了可信才能实现安全。

**可信性：**

需要时按要求执行的能力。可信性包括可靠性，可用性，恢复性，维修性，以及在某种情况下，诸如耐久性，安全性和安保等其他特性。

**国内外研究现状：**

可信计算目前的研究方向主要有以下内容：同态加密、安全多方计算、零知识证明、可信执行环境。

**从国际上来看**，可信计算技术的研究及其相关产业正在成为-一个热门的研究领域。1999年IEEE的容错专家们将容错计算学术会议改名为可信计算(Dependable Computing)会议后,便致力于可信计算的研究。目前国际上占据可信计算技术领,导地位的仍然是国际计算机软硬件领域的IT行业巨头。

**我国**在可信计算的研究方面，起步较早，水平不低。产品开发方面，2004年6月，武汉瑞达公司推出了国内首款自主研发的具有TPM功能的SQY14嵌入密码型计算机，并于同年10月通过了国家密码管委会主持的技术鉴定。该可信安全计算机是基于SSPO2芯片，采用瑞达嵌入式安全模块ESM,运用硬件的系统底层设计，结合瑞达安全增强的Linux操作系统，它极大提升了PC机的安全性，主要安全功能包括平台身份识别、平台完整性校验和芯片级的安全。2005年4月联想推出了“恒智”安全芯片，联想成为继ATLEM之后全球第二个符合TPM 1.2标准安全芯片的厂商。同年，兆日科技基于可信计算技术的PC安全芯片(TPM)安全产品也正式推出。这些产品也通过了国家密码管委会的鉴定。此后不久，采用联想“恒智”安全芯片的联想开天M40OS以及采用兆日TPM安全芯片(SSX35)的清华同方超翔S4800、长城世恒A和世恒S 系列安全PC产品纷纷面世;产品应用方面，在某省涉密网的设计中已经采用了可信计算平台，另外在金融、电信、军队、公安、电子政务领域也开始采用可信计算机来提高信息安全的整体水平。

经过近几年的不断努力,我国的安全PC产业链已初步形成，研究领域除可信终端外，还研究可信网络、可信服务器、可信接入等领域。我国也跻身世界上少数几个自主研发出可信PC的国家之列。

**2.简述你对信息安全的理解，并回答习总书记关于全球互联网发展治理的“四项原则”“五点主张”“四个共同”指的的是什么？**

**信息安全：**

计算机信息安全是由密码应用技术、信息安全技术、数据灾难与数据恢复技术、局域网组网与维护技术、数据库应用技术等技术组成的。信息安全需要满足以下特性：

(1)保密性:信息不泄露给非授权的客户、实体或者过程的特性。

(2)完整性:数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

(3)可用性:可被授权实体访问并按需求使用的特性，即当需要时应存取所需的信息。

(4)真实性：内容的真实性。

(5)可核查性：对信息的传播及内容具有控制能力，访问控制及属于可控性。

(6)可靠性：系统可靠性。

计算机信息安全范围包括：管理与技术；密码、网络攻防、信息隐藏；单机、服务器、数据库、应用系统；灾难恢复、应急响应等。

信息安全总的来说既是目标也是一门集多门学科的综合技术。信息安全的目标是保证用户信息不能被泄露，尽最大可能防止黑客等的非法入侵。

**四项原则：**尊重网络主权、维护和平安全、促进开放合作、构建良好秩序

**五点主张：**加快全球网络基础设施建设，促进互联互通；打造网上文化交流共享平台，促进交流互鉴;推动网络经济创新发展，促进共同繁荣；保障网络安全，促进有序发展;构建互联网治理体系，促进公平正义。

**四个共同：**发展共同推进、安全共同维护、治理共同参与、成果共同分享。

**3.你通过查阅文献所理解的可信与安全、可信与可靠之间的关系**

通过查阅文献明白了，可信是安全的前提条件，保证了可信才能实现安全。软件可信性则是包括了软件的可靠性，其中可信性中还包括了安全性、可用性、高效性、功能性和维护性等，它更关注使用层面的综合化的质量属性及其保障。

可靠性表示使用时间长，出现错误少，可信性包括可靠性，二者在项目中都是不可或缺的，相辅相成的关系。

**4.你通过查阅文献所理解的软件可信性属性应该包括什么（在有一个特定需求下）**

软件可信性属性包括可用性，可靠性，防危性，安全性（包括保密性和完整性），可维护性等属性。

根据国际标准化组织( InternationalOrganization for Standardization, ISO)的定义，软件质量是软件产品满足规定和隐含需求能力有关的所有特征和所有特性的总和( IEEE2标准也有类似定义)。该标准提出从内部质量、外部质量、使用质量和过程质量这四个角度来理解和保障软件质量的属性。

从软件产品自身的角度看，其质量可以通过测量内部质量属性(比如对中间产品的静态测量)，外部质量属性(比如代码执行时的特性)，或使用质量属性来评价。内部质量是软件产品内部质量属性的总和。内部质量的测量和评价用于开发阶段的非执行的软件产品(比如设计规约或源代码等)，为用户提供了测量中间制品质量的能力，从而实现预估最终产品的质量。外部质量是软件产品外部质量属性的总和。使用质量是指软件产品用于指定的使用环境和条件时，从用户角度体验到的质量。使用质量的属性包括用户在特定环境中能达到的有效性、生产率、保全性和满意度等指标，而非软件自身的性质。使用质量只能在真实的系统环境下获得。