**2021年北京邮电大学**

**《信息安全编程技术与实例开发》**

**课程设计题目及要求**

**[网络空间安全专业]**

**任课老师: 马兆丰 联系方式：**[**mzf@bupt.edu.cn**](mailto:mzf@bupt.edu.cn)

**第一部分 课程设计题目及要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **课程设计题目** | **所属类别** | **课程设计主要要求** |
| 1 | 基于同态加密的隐私数据保护系统实现 | 算法实现 | 同态加密是一种特殊的加密方法，它允许对密文进行特定的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样，它可以在加密的数据中进行诸如检索、比较等操作，得出正确的结果，而在整个处理过程中无需对数据进行解密。其意义在于，对隐私保护或受限安全访问。  研究当前已有的同态加密技术，并深入研究相关同态加密算法，等。  深入剖析并理解相关同态加密算法原理及流程，包括HEANN、NFLib、FV-NFLib、cuHE、PALISADE、HELib、SEAL等算法及相关技术。  基于Java/C语言进行上述2种算法的代码实现隐私数据（如工资或奖金）保护及应用（如比较大小，奖金高低，但不暴露数据本身），并给出正确性和有效性验证。 |
| 2 | 去中心化分布式网络安全防护系统 | 网络安全 | 根据具体情况，选定网络安全防护策略，如身份认证、单点登录、访问控制、数据访问、安全审计等策略。  基于特定安全策略，不同于传统中心化安全防护技术，实现基于区块链的分布式安全防护技术。  采用去中心化系统安全思想，基于区块链技术，公有链或许可链均可，实现基于区块链的分布式网络安全防护系统。  可采用思维导图工具建模，并基于VUE等方式实现前段设计。  可采用分布式数据库管理系统NoSQL技术如CouchDB，LevelDB,Redis技术实现数据管理。  可采用支持IPFS、P2P等方式的去中心化存储。  可采用主流先进开发技术如SpringBoot/SSM/SSH等开发框架实现程序开发。 |
| 3 | 智能终端安全通信取证系统开发 | 网络安全 | Android安全取证系统所有功能以静默形式工作，可实现证据内容的安全上传。  监控取证设备基本物理信息（包括设备型号、序列号、无线局域网地址MAC、蓝牙地址、IMEI序列号、ICCID等）。  监控取证通话记录（录音）。  监控取证短信来往。  以静默形式拨打电话、发送短信，并自动清理通话记录和短信记录。  监控取证照片内容。  监控取证IM通信活动(实时键盘记录)。  监控设备活动位置（LBS）。  将所监控取证内容进行加密存储并在空闲机时上传至特定服务器。 |
| 4 | FIDO生物认证技术实现 | 应用安全 | 研究FIDO（Fast IDentity Online）在线快速身份验证技术，并深入交接无密码的UAF(Universal Authentication Framework)和无密码的UAF(Universal Authentication Framework)技术。  研究指纹、虹视网膜或声纹认证关键技术原理。  实现指纹、虹视网膜或声纹认证中的一种。  能以较高的灵敏度进行身份认证。  具有较强的容错能力和适应性。  基于FIDO 2协议实现用户身份和设备安全进行无密码登录，保障账户安全性和便捷性。  基于Android或iOS平台实现。 |
| 5 | 区块链智能合约深度安全审计工具 | 系统安全 | 深入理解区块链智能合约技术，并熟练掌握智能合约开发工作。  针对以太坊如下合约漏洞或缺陷安全监测：智能合约调用安全漏洞、重入攻击漏洞、权限控制漏洞、数值溢出安全漏洞、账户冻结及绕过安全漏洞、逻辑设计缺陷安全问题、随机数安全误用等安全漏洞或安全缺陷。  通过智能合约安全缺陷代码和正常代码对比，增强智能合约安全编写能力。  要求基于以太坊平台进行智能合约监测和代码实现，并对能对智能合约进行3类以上安全漏洞监测。 |
| 6 | 特定环境下移动智能终端保密防护系统 | 应用安全 | 研究特定保密环境下（如位置、时间），通过特地智能终端系统功能实现，对移动智能终端相关特定功能进行致盲，使得特定功能暂时不能正常使用或开启。  实现特定时间特定环境下智能终端功能失灵，防止泄密或信息窃取等。  相关各特定功能项（包括但不限于）：拍照、录音、录像、通话、短信、网络服务等功能服务的失灵。  超出特定时段位置后，系统自动恢复相关功能。  系统及静默模式工作，具有较好的隐蔽性和安全免疫能力。 |
| 7 | 文件自动备份与强制加密系统驱动开发 | 系统安全 | 基于内核驱动技术实现文件备份与加密系统，要求先备份后加密。  实现文件备份驱动开发。  实现文件加密驱动开发。  文件在操作过程中，使用内核技术对文件系统进行扩展开发实现自动强制加密，使得文件在写操作时自动加密，在读操作时自动解密。  文件关闭时系统后台自动进行明文备份，防止发生意外损坏文件。 |
| 8 | 新型类抖音/快手 安全可信App开发 | 应用安全 | 开发一款类似抖音或快手的短视频app程序，具备主要的交互播放、点赞、评论、链接功能等。  基于区块链技术实现对视频内容的安全存证，包括内容侵权存证、违法过程存证。  基于区块链激励机制实现对内容的奖惩，做到公平可信激励与惩处。  对于用户设置不可截屏的内容防止用户截屏。  基于Android或iOS平台进行前端实现，基于Java和轻量级视频服务器实现后台数据管理和业务播放支撑。 |
| 9 | 分布式安全存储系统 | 数据安全 | 可采用不同的技术路线实现分布式安全存储系统。  实现分布式安全存储、分发、下载和共享等核心功能。  基于加密技术实现数据安全加密、隐私保护及访问控制。  完成相应分布式网络节点构建和部署。  完成代码实现和技术验证。  完成系统界面和相关数据表现形式。 |
| 10 | 去中心化数字资产发行及管理平台开发 | 应用安全 | 基于区块链技术实现数字资产发行及管理平台。  编写标准的智能合约，避免合约漏洞等安全问题。  实现数字资产的发行，资产的转账，锁仓等核心功能。  完成相应区块链网络构建和部署。  完成系统开发和代码实现。  实现基础可基于以太坊或其他技术。  系统应有完成系统界面和相关数据表现形式。 |

**第二部分 作业答疑及课程验收**

**1.答疑辅导：**课程设计相关问题需要答疑辅导，请同学们邮件、电话或微信咨询，老师给予及时响应和回复。

**2.作业提交：**课程验收前每个组长以组为单位向任课老师提交：（1）选题项目代码及执行程序；（2）项目技术内容PPT；（3）填写好的课程评分表。（4）项目材料以压缩文件提交，要求格式：XXXX项目名称-组长姓名-联系电话，验收前拷贝到老师电脑，随后由任课老师交教学主管老师留存备查。

**3.验收时间地点：**2021年09月09日（星期四）8：00-12：00， 14：00-18：00.地点：教2-339。

**4.课程验收：**课程验收按选题顺序进行，先[2018211801-2018211803]和2018211806班验收，后[2018211804-2018211805]班验收，验收时保持1-2组人员候场，验收完成的同学离场。

**5.注意事项：**作业里面需要准备并提交项目技术PPT（以备核验），**但鉴于时间紧张，课程验收时不讲PPT，只演示编程实现的代码结构及执行程序。**

**祝大家身体健康，学习进步！**

**任课老师：马兆丰 博导/硕导**

**所在学院：网络空间安全学院**

**电子邮件： mzf@bupt.edu.cn**

**电话/微信：13718841885**

**2021-08-08**