2023年信息安全/网络空间安全课程设计要求

一. 网络空间安全课程设计的题目

学生可从以下多个题目中任选一个题目，完成课程设计。

题目1：提供安全认证、加密传输和加密存储功能的网络加密磁盘空间

（1）基于网络编程技术，开发一个提供网络共享存储空间的系统。可为互联网、无线网络、移动通信等用户提供一个安全的网络存储空间。

（2）每个用户有自己的存储加密空间，支持数据和文件的加密传输和共享存储空间的本地加密存储，文件加密传输支持一次一密加密传输机制，支持防篡改和防中间人攻击。只有在共享存储空间加密存储的最初用户可以解密加密的数据，支持安全的加密数据找回机制。同时，支持多用户同时连接共享存储空间，每个用户组在共享存储空间有独立存储空间，不能登录其它用户组的空间，用户组中的用户可在多个终端登录自己的存储空间，用户组中的每个用户都可以访问用户组存储空间加密的数据并解密。

（3）每个用户登录要有安全的登录认证机制，可以采用口令、数字证书、短信、email、生物特征识别和微信/支付宝身份识别等登录认证方式中的2种登录方式进行登录，有口令找回机制。要求用户口令找回后，加密文件还可解密。

（4）用户登录认证过程中的网络传输数据需要采用加密传输机制，设计安全的密钥传输机制，支持防篡改和防中间人攻击。

（5）用户和网络磁盘空间之间，要求每次登录后的数据传输，采用自己开发实现的基于会话一次一密加密传输机制，并且网络磁盘空间中保存的数据，要求采用加密存储机制，只有创建磁盘空间的用户可以解密磁盘空间的加密数据，网盘服务器端不能解开用户加密的数据。

注：不能使用开源软件实现，不能直接调用SSL、TLS或IPSec的开源软件和函数实现。

测试环境：

在一台计算机中安装此系统，共享出一块安全的存储空间。其它计算机可从internet等有线网络、wifi、移动通信等无线网络安全登录此网络存储空间，并实现数据信息的安全传输和加密存储功能。

提示：

网络socket编程技术；

密码算法和加解密API编程技术；

对称加密算法和非对称加密算法的应用。

题目 2：基于机器学习的网络加密流量中恶意行为检测技术

收集或捕获恶意扫描或木马远程控制或漏洞攻击的加密网络数据包，通过样本分析结合机器学习的方法，按照不同类别可检测分析出加密网络数据包中的恶意行为数据包及其恶意行为分类，分析出检测的准确率和误报率。

测试环境：

Windows 或 Linux 操作系统计算机，安装所开发的基于机器学习和样本特征的加密网络流量恶意行为检测工具，可捕获离线或在线的恶意行为数据包，并进行其恶意行为检测分析分类，最后分析出检测的准确率和误报率。

提示：

学习网络协议解析；

学习机器学习算法；

学习恶意扫描或木马远程控制或漏洞攻击的典型特征。

题目 3：开源软件源代码中后门木马漏洞代码检测

针对 JAVA、Python、Go 语言的开源软件源代码，检测代码中是否存在后门、木马、漏洞等恶意代码，造成安装此类开源软件源代码并运行后，导致信息外泄或计算机被控制。

注：不能使用开源软件实现。

测试环境：

Windows 或 Linux 操作系统计算机，安装所开发的开源软件源代码后门、木马、漏洞代码检测工具，检测源代码中隐藏的恶意代码并形成检测报告，分析准确率和误报率。

提示：

学习后门木马等恶意软件代码在代码上的表现形式；

学习模式匹配、中间语言转换、向量转换等源代码检测技术。

题目 4：Android/鸿蒙系统的安全漏洞扫描和攻击控制工具

现在很多手机的 Android 系统/鸿蒙系统都存在安全缺陷，为了提高其安全性，有必要开发 Android/鸿蒙系统安全漏洞的扫描和检测工具。要求对 Android/鸿蒙系统的 app 漏洞、网络服务漏洞、系统漏洞进行漏洞安全扫描和检测，可检测应用软件、系统软件、网络服务

的漏洞，可以以自定义的标准输出模板显示检测的结果，按照漏洞的危险级别和数量进行统计并显示，能定位漏洞信息，给出漏洞的解决思路。基于 Android 系统/鸿蒙系统中的系统漏洞或应用 app 漏洞等多种漏洞，实现对手机的远程控制和文件获取。

注：Android 系统/鸿蒙系统 2 种系统可二选一。

测试环境：

自己搭建 Android 系统/鸿蒙系统的真实或模拟器环境，利用开发的安全漏洞扫描工具，可有效检测相关漏洞，并形成漏洞扫描报告。开发漏洞利用工具，实现对手机的远程控制。

提示：

学习 Android 系统/鸿蒙系统的模拟器构建

学习 Android 系统/鸿蒙系统的开发

学习 Android 系统/鸿蒙系统漏洞的原理

学习 Android 系统/鸿蒙系统漏洞的扫描检测技术和漏洞利用远控技术

二、网络空间安全课程设计组队方法

班内班间自由组合，每个题目最多 10 人组成开发小组，合作完成。

在任务分工文件中详细描述各个成员的分工。

三、网络空间安全课程设计考核方式

打包提交任务分工说明、作品技术原理介绍、概要设计报告、详细设计报告、测试分析报告、程序编译和安装使用文档、程序源代码、ppt、截屏录像。包命名方式：组长班级+组长姓名.rar/ZIP

大班学委 9 月 1 日周五将分组表发到 email：yuanjie@bupt.edu.cn 和 cuibj@bupt.edu.cn 中，或者课程导师指定的飞书目录，包括分组序号、所选题目号、组长（留手机）和组员的学号和姓名、班号，按照班号由小到大排序，答辩顺序按照组长学号顺序由小到大答辩。

9 月 7 日（周四上午 8 点）进行验收考核，地点沙河校区 N108，每组进行 15 分钟的 ppt 介绍和作品演示（每组限制时间），提前到教室来试好演示环境。考核的顺序：按照班号由小到大排序，每个班按照组长的学号由小到大为顺序先后介绍。上午 8：00－12：00，下午 1：00－全部答辩完。

9 月 8 日按照老师意见修改并完成报告，下午 18 点前提交报告至本课程指定的飞书目录。

根据小组提交程序的完成情况、完成的功能、稳定性、存在问题的多少、文档及报告完成情况、技术的合理性、技术的难度和自主性、程序的开发工作量等给予打分。

建议要求同学提前一天自行去教室测试环境和设备，保证验收时的正常演示。

四、授课老师联系方式

崔宝江 13611330827　苑洁 18911815861