

信息安全课程设计要求（2020）

一. 信息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磁盘空间

基于网络编程技术，开发一个提供网络共享存储空间。可为互联网、无线网络用户提供一个安全的网络存储空间。支持多用户同时连接，每个用户组有独立存储空间，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。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 或其它登录认证方式中的一种或 2 种登录方式进行登录，有口令找回机制。用户和网络磁盘空间之间，要求每次登录后的数据传输，采用基于会话的一次一密加密传输机制，并且网络磁盘空间中保持的数据要求采用加密存储机制。

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 等有线网络和 wifi 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：Android 安全漏洞扫描工具

现在很多手机的 Android 系统都存在较多安全缺陷，为了提高其安全性，有必要开发 Android 安全漏洞的扫描和检测工具。要求对 Android 系统进行漏洞安全扫描和检测，可检测应用软件或系统软件的漏洞，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。

测试环境：

自己搭建 Android 系统的模拟器环境，并预装有漏洞的程序，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。

提示：

学习 Android 系统的模拟器构建

学习 Android 系统的开发

学习 Android 系统漏洞的原理

学习 Android 系统漏洞的扫描检测技术

题目 3：Android/Windows10 操作系统中的远程控制软件

在 Android/windows10 系统中，开发一款远程控制软件。windows10 系统中可从客户端对服务端计算机的文件、键盘输入进行信息的获取。Android 操作系统中实现从计算机端对 Android 手机端的远程控制。针对杀毒软件特征码查杀技术应具有免杀能力。同时，考虑远程控制软件在 windows10 系统服务端和 Android 操作系统手机端的隐藏植入技术、自启动技术、自隐藏、自动网络链接，以及针对杀毒软件基于行为的主动防御功能的绕过技术。

测试环境：

两台 windows10 操作系统计算机中，或者一台 windows 操作系统计算机和一台 Android 手机服务端中，各自安装所开发的远程控制软件的客户端和服务端程序，客户端可对服务端的文件、键盘输入信息进行远程获取。在安装相关杀毒软件的条件下，对处于运行和非运行状态的远程控制软件服务端进行病毒扫描检测。

提示：

学习 Android/windows 的网络编程技术、文件和 I/O 设备的 API 接口；

学习 Android/windows 的底层编程技术、注册表 API 接口等。

利用 HOOK 技术实现操作系统中进程的监测。

题目 4：开源软件源代码中后门木马代码检测

针对 C 或 C++或 JAVA 语言的开源软件源代码，检测代码中是否存在后门木马等恶意软件代码，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。

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代码检测工具，检测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 5：基于机器学习的网络加密流量中恶意行为检测技术

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，分析检测出加密网络数据包中的恶意行为数据包及其恶意行为，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，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。

二、信息安全课程设计组队方法

班内自由组合，题目最多 8 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、信息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。包命名方式：组长班级+组长姓名.rar/ZIP

大班班长 9 月 3 日周四将分组表发到 email: yuanjie@bupt.edu.cn 和 cuibj@bupt.edu.cn 中，包括序号、组长（电话）和组员的学号和姓名、题目，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 12 日答辩开始前，每个班的学委将各自班级电子版统一拷贝或发送给苑老师 yuanjie@bupt.edu.cn。

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。

在 9 月 12 日 8:00 开始进行验收考核，地点沙河校区 N209，每组进行 10 分钟的 ppt 介绍和作品演示（每组限制时间）。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。

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。