《网络空间安全设计与实践III》

一、课程教学目的

网络空间安全设计与实践III是网络空间安全专业重要的实践性环节之一，学习本课程旨在使学生掌握坚实的网络空间安全基础理论，在密码学、网络安全、系统安全、应用安全方向具有系统的专门知识，具有较高网络空间安全综合专业素质、较强的实践能力和创新能力，能够承担科研院所、企事业单位或行政管理部门网络空间安全方面的科学研究、技术开发或管理工作。

二、教学内容及基本要求

本课程的主要教学内容是从复杂网络与系统安全、新型应用与数据安全，以及密码学的角度，针对网络空间安全常见安全问题进行综合实践演练。要求学生在网络空间安全设计与实践 I、II 的基础上，熟练应用所学网络空间安全基本原理和基本理论，培养学生综合各种技术手段，对复杂安全问题进行周密考虑、分析并予以有效解决的能力。

本课程的教学内容和教学基本要求如下：

（1）教学内容：

设计较为完整的网络应用安全通信系统，并实践协议逆向分析、软件逆向分析等安全取证技术。

（2）教学基本要求：

1）**网络与系统安全实践：**掌握 Linux、Windows 系统的安全配置方法；掌握套接口、安全套接口的基本编程方法；掌握多线程、多机通信机制；完成 C/S 通信原型系统。

2）**应用与数据安全实践：**熟练运用加密算法，掌握在线加密/解密方法，结合 1）完成加密数据多机传输的原型系统等；

3）**逆向分析技术实践：**掌握通过信息内容分析判断是否存在敏感信息方法及技术、掌握抵御命令注入攻击、脚本攻击及网站防篡改技术等 web 安全技术，结合计算机网络及信息内容安全课程，运用逆向工具分析上述系统运行过程中的网络通信数据，并编写程序。

三、课设内容及要求

- **课设内容**

本次课设分三个阶段，分别打分：

第一阶段：Diffie-Hellman 协议的实现

1、客户端与服务器之间通过 TCP Socket 通信；

2、客户端与服务器之间通过 Diffie-Hellman 协议协商出对称密钥；

3、客户端使用协商出的对称密钥对传输内容做加密，并发送给服务端；
4、服务端接受客户端发送过来的内容，进行解密；
5、对称加密算法采用 AES256-GCM；

第二阶段：Diffie-Hellman 中间人攻击方法研究与实现

6、研究 Diffie-Hellman 协议，研究中间人攻击方法并完成相关代码。当通信双方进行通信时，中间人攻击程序可以解密出传输内容；

第三阶段：Diffie-Hellman 协议改进

7、基于预共享密钥的方式对 Diffie-Hellman 做改进，使协议抵抗中间人攻击。完成协议设计，实现代码并用第 2 阶段的中间人攻击程序做验证；

■ **课设要求**

1、课程设计必需在 Linux 系统上开发，开发语言必需为 C 语言；
2、2 人一组完成；
3、验收时按照现场验收评分表进行打分。

四、课设报告要求

1、概要设计：说明设计中用到的所有抽象数据类型的定义,主程序的流程以及各程序模块之间的层次(调用)关系.技术开发思路

2、详细设计：实现概要设计中定义所有数据类型，绘制流程图及关键技术实现伪码。

3、调试分析：调试过程中遇到的问题并且是如何解决的以及对设计实现的回顾讨论和分析;经验和体会及改进设想。

4、测试结果：列出测试结果,包括输入的数据和相应的输出数据图示.

5、附录：应附上带详细注释的源程序.

请班长在 7 月 5 日将课程设计报告（纸质版）送交双创园 1 号楼 605 室，电子版发至 lyylwhhit@126.com，文件夹命名方式为学号+姓名，内容包括：课程设计报告、源码、程序运行界面及结果展示（Word）。

四、成绩评定标准

理论设计方案,演示所设计的系统,总成绩 30%;设计报告,占总成绩 60%;考勤情况,占总成绩 10%;

说明：每人独立完成所分配的任务，单独评定成绩，不能抄袭。课程设计报告须提交运行文件及完整文档。

网络空间安全设计与实践III
课程设计现场验收评分表

小组成员组成				
1	学号		姓名	
2	学号		姓名	

小组得分情况				
序号	项目	内容	分值	得分
1	开发能力	程序支持命令行参数	4	
2		源代码使用 Makefile 或 cmake 编译	2	
3		源代码拆分成多个文件	2	
4		开启编译器优化	2	
5		程序支持后台运行	3	
6		源代码使用 git 进行版本管理	3	
7		代码风格良好	3	
8	软件功能	第一阶段程序功能	12	
9		第二阶段程序功能	16	
10		第三阶段程序功能	14	
11	附加得分	其它有亮点的附件功能	9	