《软件安全》教学大纲

课程编号： CE5102

课程名称： 软件安全　　英文名称：software security

学分/学时：3/32+32　　课程性质：必修

适用专业： 信息安全、网络空间安全　　建议开设学期：6

先修课程： 操作系统原理及安全、编译原理

开课单位：网络与信息安全学院

一、课程的教学目标与任务

本课程是信息安全学科的本科专业选修课，拟采用核心知识讲解、学生自学及课堂互动相结合的方式授课。本课程旨在增强学生对目前软件安全所面临的各类威胁的本质及其实现机理的理解，促使学生掌握目前系统安全防护领域的各类核心技术与理论，以提升学生的实践创新能力和学生综合利用专业基础知识来设计和研发信息安全产品的能力。

二、课程具体内容及基本要求

（一）软件安全基础(6 学时)

一、计算机存储空间原理

- Windows/Linux 操作系统中进程的内存布局
- 虚拟地址及其转译
- 操作系统对内存的分配和管理

二、指令系统

- 数的机器编码及表示
- 指令系统的基本概念
- 8086/8088 指令系统初步

1. 基本要求

（1）掌握主流操作系统环境下的进程内存布局；

（2）熟悉虚拟地址转译的原理；

（3）了解数的几种主要的机器编码和表示方法；

（4）熟悉 8086/8088 指令系统，掌握其核心编码规则。

2. 重点、难点

重点：操作系统的内存布局、虚拟地址转译、以及 8086/8088 指令系统的编码规则为此部分重点。

难点：数的机器编码和表示方法、8086/8088 指令系统的编码为此部分的难点所在。

3. 作业及课外学习要求：

要求学生在课外进行扩展阅读，了解 iOS、Android 等主流移动操作系统平台下应用程序的内存布局，以及 JAVA 字节码的解释执行原理与 8086/8088 等二进制代码之编译执行原理的区别。

此外，要求学生在不依赖自动化工具的前提下，通过查阅手册等方式写出指定的 8086/8088 指令所对应的二进制形式，作为一次作业。

（二）软件漏洞利用与防护(14 学时)

一、缓冲区溢出类漏洞

- 栈溢出的原理
- 进程的堆空间的构造和堆结构的维护
- 堆溢出的原理
- 越界访问类漏洞及其与缓冲区漏洞的异同

二、格式化字符串漏洞和类似的 Web 攻击

- 格式化字符串漏洞的原理和潜在的后果
- SQL 注入漏洞的原理及其利用方式
- 跨站脚本和跨站请求伪造

三、软件漏洞的利用

- 代码注入及其 Shellcode 的寻址实现方式
- Ret2Libc 和返回导向编程(ROP)等前沿 Shellcode 编码的原理
- 返回导向编程的演进和变种

四、操作系统安全机制及漏洞防护技术

- 漏洞挖掘技术的基本类别
- 主流操作系统针对代码注入的防护机制
- 现有的栈溢出检测方法及其不足之处
- 地址空间随机化(ASLR)的原理、缺陷以及针对 ASLR 的攻击手段
- 控制流完整性保护(CFI)的基本思想、前沿方法和根本性弱点

1. 基本要求

（1）掌握各种缓冲区溢出漏洞的原理；

（2）掌握 SQL 注入的原理，了解跨站脚本、跨站请求伪造；

（2）掌握 ROP 等前沿 Shellcode 编码方法；

（3）熟悉主流操作系统针对代码注入的保护机制；

（4）熟悉栈溢出检测方法及其不足；

（5）熟悉 ASLR、了解现有 ASLR 技术所存在的问题；

（6）了解 CFI 技术的原理、当前发展趋势及核心不足所在；

（7）了解漏洞挖掘技术的分类和基本工作原理；

（8）了解 ROP 技术在 ASLR、CFI 等防护手段出现的背景下产生的演进。

2. 重点、难点

重点：缓冲区溢出漏洞、格式化字符串漏洞和 SQL 注入、以 ROP 为代表的新型 Shellcode 编码、ASLR 和 CFI 等针对 ROP 的防护机制等为此部分重点。

难点：堆的结构及维护、堆溢出漏洞、ROP 的原理和应用、CFI 的缺陷、针对 ASLR 的前沿攻击方法等为此部分的难点所在。

3. 作业及课外学习要求：

要求学生利用栈溢出和基本的 ROP 编码方法、就指定的高级语言算法写出对应的 Shellcode，作为一次作业。

（三）恶意代码的机理及其防护(4 学时)

一、传统恶意代码

- 计算机病毒的特点、主要类型与传播方式
- 网络蠕虫的结构及其所涉及的关键技术
- 木马的概念、木马与远端的通信方式、木马与后门的区别

二、Rootkit 与智能手机恶意代码

- Rootkit 的基本概念与核心技术
- 智能手机恶意软件基础及其前沿发展趋势
- 重包装攻击及其与智能手机恶意软件的关系

三、恶意代码的检测与防护

- 恶意代码的潜在载体、恶意代码样本的捕获
- 前沿的恶意代码检测技术与重包装攻击检测方法介绍

1. 基本要求

（1）了解传统恶意代码的种类、特征和工作机理；

（2）了解 Rootkit、智能手机恶意软件和重包装攻击；

（3）了解恶意代码的捕获、检测和分析技术。

2. 重点、难点

重点：软件漏洞与网络蠕虫的关系、木马与后门的区别、Rootkit 及其核心技术等为此部分重点。

难点：Rootkit 及其核心技术、恶意代码的检测分析技术及其前沿等为此部分的难点所在。

3. 作业及课外学习要求：

要求学生自行设计并实现一个无害的网络蠕虫，或自选一种已知的 Android/iOS 系统 Rootkit 并分析其工作原理，作为一次作业。

（四）软件自我保护(8 学时)

一、软件自我保护综述

- 传统的软件自我保护机制概述
- MATE 攻击的概念、所依赖的技术和工具及其与软件漏洞利用的区别
- 用于对抗 MATE 攻击的软件自我保护技术的主要分类

二、代码混淆

- 代码混淆概念和作用
- 代码混淆的对象
- 代码混淆的“虚拟黑盒”安全目标及其不可能性
- 现存的前沿代码混淆方法的原理及其不足之处

三、软件防篡改

- 软件防篡改的安全目标及其与代码混淆的区别
- 现有软件防篡改技术及其主要问题所在

四、软件水印

- 软件水印的概念、软件水印与一般的数字水印的异同
- 软件水印的主要分类
- 前沿软件水印设计简介以及软件水印技术目前尚无法解决的问题

1. 基本要求

（1）熟悉 MATE 攻击的概念、目标和所依赖的手段；

（2）熟悉代码混淆、软件防篡改和软件水印技术的基本概念和安全目标；

（3）掌握代码混淆的“虚拟黑盒”安全目标的不可能性证明过程；

（4）了解现有软件保护技术及其存在的不足。

2. 重点、难点

重点：MATE 攻击的概念、代码混淆“虚拟黑盒”这一安全目标的不可能性证明、现有代码混淆和软件水印技术及不足等为此部分重点。

难点：“虚拟黑盒”安全目标的不可能性证明为此部分的难点所在。

3. 作业及课外学习要求：

要求学生在指定目标软件上亲手实现一种现有的代码混淆或软件水印方法，作为一次作业。

三、教学安排及方式

总学时 32+32 学时，其中：讲授 32 学时，实验 32 学时。

序号	课程内容	学时	教学方式
1	计算机存储空间原理	4	讲授
2	指令系统	2	讲授
3	缓冲区溢出漏洞	2+4	讲授+实验
4	格式化字符串漏洞	2+4	讲授+实验
5	Web 应用程序漏洞	2+2	讲授+实验
6	软件漏洞的利用	4+6	讲授+实验
7	操作系统安全机制及漏洞防护技术	4+6	讲授+实验
8	恶意代码及 Rootkit	2	讲授
9	恶意代码的检测与防护	2+2	讲授+实验
10	软件自我保护综述	2	讲授
11	代码混淆、软件防篡改	3+4	讲授+实验
12	软件水印、软件胎记	3+4	讲授+实验
		32+32	

四、本课程对培养学生能力和素质的贡献点

通过本课程的学习，学生可系统地了解软件安全所面对的主要威胁，熟悉各种软件保护机制和技术的基本原理，熟悉各类恶意代码的特征及相应的检测技术，掌握典型的软件漏洞利用方法。这将使学生能够充分地掌握和运用前沿的软件防护、恶意代码检测、漏洞挖掘等方法和手段，为学生从事软件和操作系统安全防护工作打下坚实的基础。学习本课程后，学生应具备如下能力：

1.掌握软件安全的基础知识，具有软件攻防相关的系统实践经历，了解软件安全的前沿发展现状和趋势；

2.面对软件漏洞，具备构造和实施各种基本 Shellcode 的能力，并能够自主实现简单的恶意代码，从而对软件安全所面对的威胁拥有切身、深刻的理解；

3.掌握基本的软件防护方法设计与创新方法，具有追求创新的态度和意识；具有综合运用理论和技术手段设计防护机制和系统的能力；

4.通过了解软件安全技术的发展历程，对终身学习有正确认识，具有不断学习和适应发展的能力。

知识、能力、素质矩阵：1.工程知识(M)；2.问题分析(M)；3.设计/开发解决方案(M)；5.使用现代工具(M)；6.工程与社会(M)；12.终身学习(L)。

<table>
<tr><th>毕业要求能力点</th><th>对应教学内容</th><th colspan="2">考核方式及达成评价</th></tr>
<tr><td>毕业要求 1：
工程知识(M)</td><td>全部教学内容</td><td colspan="2"></td></tr>
<tr><td>毕业要求 2：
问题分析(M)</td><td>教学内容 3、4 、 5 、 6 、10、11</td><td colspan="2"></td></tr>
<tr><td rowspan="2">毕业要求 3：
设计/开发解决方案(M)</td><td>教学内容 3、4、6、7、9、10、11</td><td>考核方式：
课后作业/书面考试</td><td>达成评价：
H：课后作业完成度高于 60%（含）
E：期末考试综合成绩高于 60 分</td></tr>
<tr><td>教学内容 3、4、6、7、9</td><td>考核方式：
上机实验</td><td>达成评价：
T：上机练习独立完成度高于 60%（含）</td></tr>
<tr><td>毕业要求 5：
使用现代工具(M)</td><td>教学内容 6、7 、 8 、 9 、10、11</td><td>考核方式：
上机实验</td><td>达成评价：
T：上机练习独立完成度高于 60%（含）</td></tr>
</table>

毕业要求 6： 工程与社会(M)	教学内容 3、4、5、6、8、10、11	
毕业要求 12： 终身学习(L)	全部教学内容	

五、考核及成绩评定方式

最终成绩由平时作业成绩、期末成绩组合而成。各部分所占比例如下：

日常考勤：20%。主要考察学生的日常听课状况。

平时作业成绩：30%。主要考核对软件安全课程每章节知识的理解、掌握程度，并考察学生参与课程学习的积极性。

期末考试成绩：50%。主要考核软件安全基础知识的掌握程度以及基本的应用能力。书面考试形式。题型为问答题和计算题等。

六、教材及参考书目

教材：《软件安全》，彭国军，傅建明，梁玉著，武汉大学出版社

参考书目：

1.《软件安全：从源头开始》，[美]詹姆斯·兰萨姆，安莫尔·米斯拉著，丁丽萍译，机械工业出版社

2.《漏洞战争：软件漏洞分析精要》，林桠泉著，电子工业出版社

3.《软件加密与解密》，[美] Christian Collberg，Jasvir Nagra 著，崔孝晨译，人民邮电出版社

2017 年 10 月 21 日