软件安全与威胁

一、 课程背景

近年来，我国互联网蓬勃发展，网络规模不断扩大，网络应用水平不断提高，成为推动经济发展和社会进步的巨大力量。与此同时，网络和业务发展过程中也出现了许多新情况、新问题、新挑战，尤其是当前网络安全问题频发、网络安全立法系统性不强、及时性不够和立法规格不高，物联网、云计算、大数据等新技术新应用、数据和用户信息泄露等的网络安全问题日益突出。未来，我国将不断加强网络安全依法管理、科学管理，更加重视新技术新应用安全问题，促进移动互联网应用生态环境优化，加速构建网络安全保障体系，推动网络安全相关技术和产业快速发展。

本课程通过教师讲解、案例分析、小组讨论、互动等授课方式，给学员系统的讲解软件安全知识，带来全面的认识和思考，让软件安全技术的学习变得妙趣横生。整个课程主要先让大家认识什么是信息和信息安全，再由网络攻击现状过渡到现实生活中企业如何在系统开发阶段就加入安全要素，使学员深刻理解软件安全的现实运用。

课程将通过大量的案例分析，介绍国内外对于软件安全这门技术的应用和深入情况，使学员在理解了软件安全这一概念后思维能够从理论性的阐述中逐渐联系实际应用，以此全面了解网络安全，使之贴合，做到理论和实际能紧密联系，有效运用。

二、 课程特点

授课形式：理论讲解+案例分析+小组讨论+互动答疑

突出理论特点，注重知识理解、案例分析与小组讨论，其中理论讲解 60%，案例分析 30%，讨论 10%。

三、 课程收益

1. 详细了解信息安全、网络安全的概念和体系。
2. 详细了解软件安全威胁。
3. 详细了解软件威胁建模。
4. 详细了解安全需求分析。
5. 具备从网络空间安全视角看待行业未来的发展的能力，理解网络空间安全在行业运用中的关键。

四、 课程模式

1. 中文教学、面授
2. 理论讲解
3. 案例分析
4. 互动式答疑

五、 受众对象

1. 项目经理、开发人员
2. 管理支持组织中复杂工作、重要工作的人员
3. 希望提升自身职业能力的人员、其他对软件安全感兴趣的人员

六、 时间安排

总学习时间为 5 天

七、 授课教师

芦效峰，北京邮电大学软件安全中心副主任，
网络空间安全学院副教授，硕士生导师
EXIN 认证云计算专家，
微软认证专家，
CCNA 讲师

八、 课程内容

软件安全与威胁

第一阶段 软件安全意识 1 天

第一章　信息安全基础与保障

时长 3 小时

- 信息安全背景与原理
- 典型信息系统安全模型与框架
- 信息安全保障工作概况
- 信息安全保障工作基本内容

第二章　软件安全基础

时长 3 小时

1. **软件安全**
   - 软件安全现状
   - 软件安全概念
   - 软件安全的属性
2. **软件漏洞**
   - 软件漏洞对系统的危害
   - 软件漏洞产生的原因
   - 改善软件的安全属性
3. **软件安全开发生命周期**

第二阶段 安全模式进阶 1 天

第三章　网络安全技术

本节要点：网络攻击防御的方法，时长 3 小时

1. **防火墙**
   - 防火墙概述
   - 防火墙技术
   - 防火墙的体系结构

2. **入侵检测技术**
   - 入侵检测系统概述
   - 入侵检测系统的分类及技术
   - 入侵检测系统的实施
3. **VPN**
   - 概念
   - 功能
   - 隧道技术
   - VPN 类型
   - 网络层 VPN：IPsec
   - 应用层 VPN：SSL

第四章　密码学基础和访问控制

本节要点：介绍密码学知识和访问控制，时长 3 小时

1. **密码学**
   - 对称加密
   - 非对称加密
   - 密码的管理和分配
   - 数字证书
   - 数字签名
2. **访问控制**
   - 访问控制模型
   - 访问控制技术

第三阶段　安全威胁进阶 1 天

第五章　安全威胁

时长 3 小时

1. **STRIDE 威胁模型**
   - 假冒
   - 篡改
   - 否认
   - 信息泄露
   - 拒绝服务
   - 权限提升
2. **Web 安全威胁**
   - SQL 注入

- 输入确认
- XSS
- 跨站请求伪造

3. **缓冲区溢出**
4. **恶意软件**
   - 病毒
   - 木马
   - 蠕虫
   - 僵尸

第六章　威胁建模

时长 3 小时

1. **威胁建模**
   - 系统的威胁建模方法
   - 软件模型
   - 发现威胁
   - 攻击树
   - STRIDE 变种

第四阶段　安全软件设计 1 天

第七章　安全软件开发模型

本节要点：一般软件开发模型和微软 SDL，时长 3 小时

1. **软件开发模型**
   - 软件开发模型
   - 瀑布模型
   - 原型模型
   - 增量模型
   - 敏捷模型
2. **微软安全开发模型 SDL**

第八章　安全设计与威胁防御

本节要点：介绍软件安全设计指导原则，时长 3 小时

1. **软件安全指导原则**
   - 纵深防御
   - 最小权限
   - 多因素
   - 隐私保护
2. **软件架构安全**
3. **威胁防御**
   - 减缓威胁
   - 解决威胁的策略
   - 验证威胁是否解决

第五阶段 安全软件开发 1 天

第九章 安全开发与自我保护

本节要点：介绍软件安全测试知识和保护知识，时长 3 小时

1. **软件安全开发**
   - 软件安全编码
   - 软件安全测试
2. **客户端安全**
   - 静态分析对抗
   - 动态分析对抗

第十章 总结与技术交流