1. Fundamentals of Information Security
   - Introduction to Information Security 信息安全介绍
   - Cryptographic Techniques 加密技术
   - Authentication Techniques 认证技术
2. Internet Security
   - Introduction to Internet Security 因特网安全介绍
   - Network Attack and Defence 网络攻击和防御
   - Firewall 防火墙
   - Intrusion Detection & Protection 入侵检测和保护
3. Web Security
   - The Architecture and Security of Web Applications web 应用架构和安全
   - Security Flaws of Web Applications Web 应用的安全缺陷
   - Secure Web Programming 安全网络编程

- Module I. Fundamentals of Information Security
  - Chap 1. Introduction to Information Security
    - Concepts of Information Security 信息安全概念
      - Situation of Information Security: Security situation report from CNCERT/CC 【中国国家互联网应急中心】 信息安全现状
      - Definition of Information Security: security, information security, computer security and information assurance 信息安全的定义：安全性，信息安全
      - History of Information Security
      - Key Concepts: CIA triad【保密性、完整性、可用性】 and others【真实性，保密性…】
    - Computer System Security 计算机系统保密安全性
      - Computer System Vulnerabilities 计算机系统脆弱性
      - Terminology（术语）: Adversary (Threat agent，敌方)，Attack (攻击)，Countermeasure (对策)，Risk (风险)，Security Policy (安全策略)，System Resources (Asset，信息资产)，Threat (威胁)
      - Threat Consequence：Unauthorized Disclosure 泄露 ，Deception 欺骗 ，Disruption 搅扰/破坏，Usurpation 篡夺
      - Operating System Security 操作系统安全: 进程隔离和内存管理，用户权限管理，访问监控器，可信计算基
      - Database Security 数据库系统安全
      - User Application Security 用户应用安全
    - InfoSec Service, Management and Audit 信息安全服务，管理和审计
      - Information Security Services 信息安全服务
        - Concept of Information Security Service
        - Authentication 认证
        - Access Control 访问控制
        - Confidentiality 保密性
        - Integrity 完整性
        - Availability 可达性
        - Non-repudiation 不可抵赖性
      - Information Security Management 信息安全管理
      - Information Security Audit 信息安全审计
      - Levels of Information Security: GB/T 20269-2006 信息安全管理五个等级
    - Conclusion
      - Levels of Impact – Low, Moderate, and High
      - Three Aspects of Information Security 信息安全的三个方面
        - Security attack （Passive Attack & Active Attack）安全攻击（主动&被动）
        - Security mechanism (control) 安全机制（控制）

        - Security service 安全服务
    - Attack Surface 攻击截面
    - Attack Trees
    - Fundamental Security Design Principles 基础安全设计原则
    - Balancing Information Security and Access 平衡信息安全和可用性
    - Information Security Implementation 信息安全实现
    - The Security Systems Development Life Cycle （SecSDLC）
    - Discipline System of Information Security
    - 信息安全等级保护标准体系

■ Chap 2. Symmetric Cryptographic System 对称加密系统
- Introduction to Cryptology 密码学
    - Definitions, Kerckhoffs' Principle, Shannon's Maxim
    - Cryptanalysis 密码分析学，密码分析的常用方法
    - History of Cryptology 历史
    - Concepts & Items 概念
    - Cryptosystems 密码体制
    - Shannon's Condition 强加密算法的特性 Attributes of Strong Encryption，也称香农条件
    - Management of Cipher Keys 密钥管理
- Symmetric Key Cryptographic Algorithms 对称加密算法
    - Introduction of Symmetric Cryptography
    - Algorithm Types & Modes: stream and block cipher【流加密和块加密】, ECB, CBC, CFB,OFB
    - Data Encryption Standard (DES) 数据加密标准
    - Advanced Encryption Standard (AES)

■ Chap 4. Asymmetric Cryptographic System 非对称加密系统
- Introduction
- Knapsack Problem and MH Algorithm 背包问题和 MH 算法（基于背包问题的公钥密码系统）
- Diffie-Hellman Key Exchange Algorithm 密钥交换算法
- The RSA Algorithm
- Generating Big Primes 大素数生成
- RSA for Digital Signature 数字签名

■ Chap 5. MAC and Hashing Algorithms 消息认证码 MAC 和哈希算法
- Introduction
    - 消息认证的方式（消息认证加密方法，消息认证码，哈希法，数字签名）
- Message Authentication Code 消息认证码
    - Concept of MAC
    - MAC Algorithm：ANSI x9.17 标准（FIPS PUB 113）
- Hash Method 哈希方法
    - Concept of Hash Method
    - Hash Function：分类，对散列方法的攻击
- MD5 Algorithm 【信息-摘要算法 5】
- Other MD Algorithms
    - SHA
    - RIPEMD
    - HMAC
- Digital Signature 数字签名

- Chap 6. Authentication and Kerberos
  - Introduction
    - Authentication Technologies
    - The Weak/Strong Authentication Scheme
    - Zero-knowledge Authentication & Fiat-Shamir Algorithm
    - The Application of Authentication Technologies
      - X.509
      - Kerberos
    - Attack to Authentication
    - The Security Guidelines to Protect Authentication Schemes 验证方案
  - Public Key Infrastructure 公钥基础设施
    - Introduction to PKI
    - PKIX (Public key infrastructure X.509)
    - Public Key Certificate 公钥证书
    - Trust Hierarchy Model 可信分层模型
  - Kerberos
    - Introduction
    - The Needham-Schroeder symmetric key protocol
    - Kerberos Process
    - Drawbacks & Limitations
  - X.509
    - X.509 Certificate
    - Security problems
    - Application

- Module II. Internet Security
  - Chap 7. Network Security Architectures
    - Overview
      - International Standards Organizations 国际标准组织
      - Layers of Network Security Architectures 网络安全架构的五个层次（物理环境，操作系统，网络，应用，管理）
    - Information Security Models 信息安全模型
      - Secure OS 安全操作系统
      - TCSEC, BS 7799 and CC Criteria 信息安全评估标准
      - Access Control Models 访问控制模型
      - PDR, P2DR and PDRR Models 入侵检测模型
    - Information Assurance 信息保障
      - Information Assurance System 信息保障体系
      - IATF 信息保障技术框架
    - OSI Secure Architecture 开放式计算机网络层次结构参考模型
      - ISO 7498-2:1989/OSI Security Architecture
        - 安全生命周期
        - 安全威胁、安全服务、安全机制
        - 安全域、安全策略
        - 威胁，脆弱和风险分析
        - 安全措施分类
      - OSI Security Services OSI 安全服务：认证、访问控制、数据保密性、数据完整性、抗抵赖性
      - OSI Security Mechanisms OSI 安全机制
    - ITU-T X.800 and Others
      - X.800

- Security Functional Requirements 安全功能需求
- NSTISSC Security Model

- Technology and Principles 技术和原则
- Protocols and Standards 协议和标准
  - 安全管理框架
  - 安全技术标准
  - 安全产品标准
  - 安全工程标准
  - 安全方法论
  - 安全资格认证
- Web Security
  - A Secure Architecture for Web Applications Web 应用安全架构
  - Apache, IIS【互联网信息服务】 and Other Web Servers
  - QWASP Top 10, 2017 最严重的 Web 应用安全风险
  - Web Services Security Frame
  - Threats/Attacks Organized By the Web Services Security Frame
  - Guidelines: Improving the Security of Web Services

■ Chap 8. IPSec and SSL

- IPSec
  - Introduction
  - 为什么要保护数据，IPSec 如何保护数据
  - Some Basic Concepts about IPSec： AH,ESP,隧道/传输模式
  - ESP protocol 封装安全载荷协议
  - IKE【因特网密钥交换】 - Key Management of IPSec
  - Gateway and Road Warrior Mode 两个网关/一头网关，一头单个客户端
- SSL/TLS
  - Introduction
  - How TLS Works
  - Decryption of TLS Packet
- VPN 虚拟私有网络
  - Introduction to IPsec VPN
  - OpenVPN 传输层，SSL 协议

■ Chap 9. Network Attack and Defense 网络攻击与防御

- Introduction
  - Network Security Crisis 网络安全危机: cyberspace 网络空间 and cybersecurity 网络空间安全; virus, worm and Trojan 病毒，蠕虫和木马; cyberspace ecology deterioration 信息生态恶化
  - Hacking & Hackers: activities of hacking
  - Network Threats: internal threats, unstructured external threats and structured external threat
  - Steps of Network Attack
  - Methods of Network Defense
- Network Attacks 网络攻击
  - Consequences of Cyberattacks 后果
  - Types of Network Attack 类型: Eavesdropping 窃听, Data Modification 数据篡改, Identity Spoofing (IP Address Spoofing) 身份欺骗,Password-Based Attacks 盗用口令攻击, Denial-of-Service Attack (DoS)拒绝服务攻击,Man-in-the-Middle Attack (MITM) 中间人攻击, Brute Force Attack 暴力破解攻击,Compromised-Key Attack (盗取密钥攻击), Sniffer Attack 嗅探器攻击, Application-Layer Attack 应用层攻击
  - Port Scan 端口扫描: NMap & SuperScan; TCP scanning, SYN scanning, UDP scanning, ACK scanning, FIN scanning

- Process of Idle Scanning 空闲扫描
- Password Cracking 密码破解
  - The Vulnerability of Passwords
  - Password Selection Strategies
  - Password Cracking
  - Useful Tools: top 10
- Buffer Overflow 缓冲区溢出
  - Background: process virtual memory 进程虚拟地址空间, layout of the virtual address space on IA-32 (Intel Architecture 32-bit)
  - Stack Overflow and Heap Overflow
  - Practicalities
  - Protection: Safer Language, Libsafe, Canary Value, Address Space Layout Randomization, Non-executable Program Memory
- Spoofing Attack 欺骗攻击
  - ARP Cache Poisoning ARP 缓冲区毒化
  - DNS Spoofing
  - Web Spoofing
  - IP Spoofing: Mitnick attack

■ Chap 10. Firewalls

- Introduction
  - Definition and Classification of Firewalls 防火墙的定义和分类
  - 防火墙的作用
  - Functions & Deployment of a Firewall
- Packet Filtering Firewall 包过滤防火墙
  - What is Packet Filtering Firewall 是什么
  - How Packet Filtering Firewall Works 怎么工作
  - Advantages & Disadvantages 优缺点
  - Attacking Packet Filtering Firewall 攻击它
- Stateful Inspection Firewall 状态检测防火墙
  - What is Stateful Inspection Firewall 是什么
  - How Stateful Inspection Firewall Works 怎么工作
  - Advantages & Disadvantages 优缺点
  - Attacking Stateful Inspection Firewall 攻击它
- Application Proxy Firewall 应用网关防火墙（应用层代理）
  - What is Proxy 是什么
  - Topological Graph of Proxy
  - Functions Offered by Proxy 作用
  - Advantages & Disadvantage 优缺点
  - Attacking Proxy 攻击它
- Bastion Host 堡垒主机
  - Bastion Host
  - Entrance Control Host 进入控制堡垒主机
  - Internal Control Host 内控堡垒主机
  - Deployment of Bastion Host 堡垒主机的物理部署
- Iptables
- Conclusion
  - Attacks to Firewalls 黑客对防火墙攻击类型
  - Limitations 防火墙的局限性

- Vulnerabilities 防火墙的脆弱性
- Hardware Firewall 硬件防火墙
- Software Firewall 软件防火墙

Chap 11. Intrusion Detection 入侵检测

Introduction to IDS

- Threats to Computer System（DoS、Spoofing、Eavesdrop 窃听、Password Cracking、Trojan 木马、Others）
- Process of Intrusions 入侵的过程
- What Is Intrusion Detection 入侵检测：Intrusion 入侵行为，Audit 审计，Intrusion Detection 入侵检测，Intrusion Detection System, IDS 入侵检测系统，入侵检测系统的作用，IDS vs 防火墙
- Methods of Intrusion Detection ： Anomaly Detection 异常检测，Misuse Detection 误用/滥用/盗用检测

Framework of IDS 入侵检测系统框架

- Basic Structure of IDS ： Information Gathering 信息收集，Analysis Engine 分析引擎，Response Unit 响应单元，IDES 入侵检测专家系统，CIDF 通用入侵检测框架
- Host-Based IDS (HIDS) 基于主机的 IDS
- Network-Based IDS (NIDS) 基于网络的 IDS
- HIDS vs. NIDS

Intrusion Prevention System 入侵防御系统

- The Need of IPS：IDS 不能完全满足安全目标的需求
- Security Capabilities 安全功能：检测入侵，阻止入侵，报告入侵
- Types of IPS：基于主机的入侵防御系统 HIP，基于网络的入侵防御系统 NIPS
- IPS vs. IDS

Module III. Web Security

Chap 12. Security of Web Applications

Overview

- Web Applications：Web 的组成部分【服务器端、客户端、通讯协议、Web 应用】
- C/S and B/S Models 客户端-服务器，浏览器-服务器，Web 应用结构
- Web Site Architecture Web 网站架构: hardware 硬件架构, 3-tiers software 软件的三层逻辑架构, MVC
- Electronic Commerce Architecture 电子商务架构
- Apache & IIS Web Server: Netcraft web server survey

SOA (Service-Oriented Architecture 面向服务架构)

- Concept of SOA
- Oracle's SOA

Web Services Web 服务

- Overview（W3C,模式：【RPC,SOA,REST】,协议：【XML,SOAP,WSDL,UDDI,RPC】
- SOAP

Web Security Primer Web 安全入门

- Web Security – Beginning: why not secure Web 安全问题的原因, Web 安全问题的三大目标，Web Security Technology Web 安全技术, Web Security Flaws Web 应用的安全漏洞
- Web Server Vulnerabilities Web 服务器脆弱性，Threats to Web Server Web 服务器安全威胁
- Web Services Secure Model Web 服务安全模型: WS-Security、 WS- Policy、WSTrust
- Prevention of Malicious Codes
- SSL/HTTPS