中山大學
SUN YAT-SEN UNIVERSITY

SYLLABUS

2018-1 (Fall 2018)

Class Hours: 10:00-11:40 Wed. / C305 (Week 1-18)

Lecture Notes: courseware_is_sysu@163.com
Instructor: Cai Guoyang, email: isscgy@mail.sysu.edu.cn

Web Security: *Principles & Applications*

School of Data & Computer Science, Sun Yat-sen University

Syllabus - Description

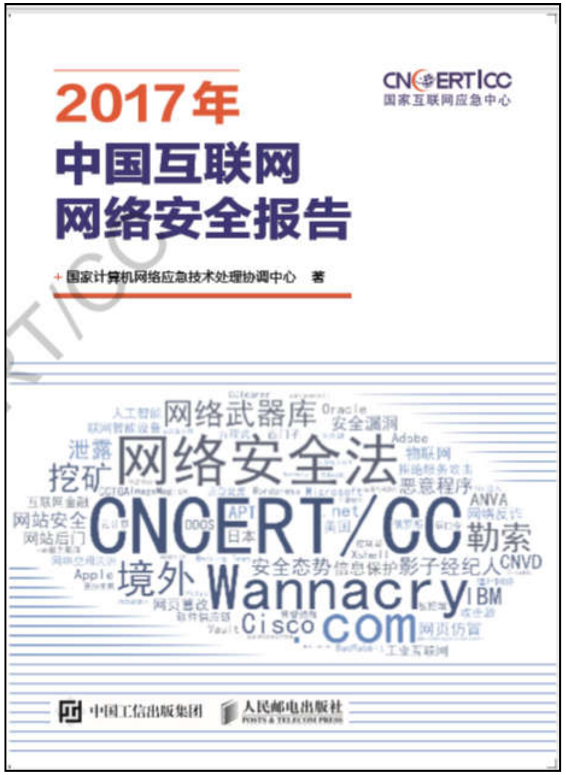
- **A. DESCRIPTION**
  - The Importance of Information Security
    - ✧ 《中华人民共和国网络安全法》于2017年6月1日起施行
    - ✧ 工学一级学科：网络空间安全 Cyberspace Security (2017)
      - ◌ 网络空间安全研究所
      - ◌ 信息安全重点实验室、工业控制信息安全重点实验室
    - ✧ Cyberspace
      - ◌ Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography.
      - ◌ *William Gibson* is sometimes credited with inventing or popularizing the term by using it in his novel of Burning Chrome,1982 and Neuromancer, 1984.

Syllabus - Description

- **A. DESCRIPTION**
  - The Importance of Information Security
    - ✧ 网络空间安全 (Cyberspace Security)
      - ○ 网络空间是信息环境中的一个整体域，它由独立且互相依存的信息基础设施和网络组成。包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统。
      - ○ 网络空间安全研究网络空间中的信息在产生、传输、存储、处理等环节中所面临的威胁和防御措施，以及网络和系统本身面临的威胁和防护机制。网络空间安全不仅包括传统信息安全所研究的信息的保密性、完整性和可用性，还包括构成网络空间的基础设施的安全和可信。
      - ○ 网络空间既是人的生存环境，也是信息的生存环境，人在其中与信息相互作用、相互影响。网络空间安全是人和信息对网络空间的基本要求。

Syllabus - Description

- **A. DESCRIPTION**
  - The Importance of Information Security
    - ✧ CNCERT/CC Annual Report 2017
    - ✧ OWASP Top 10 For 2017



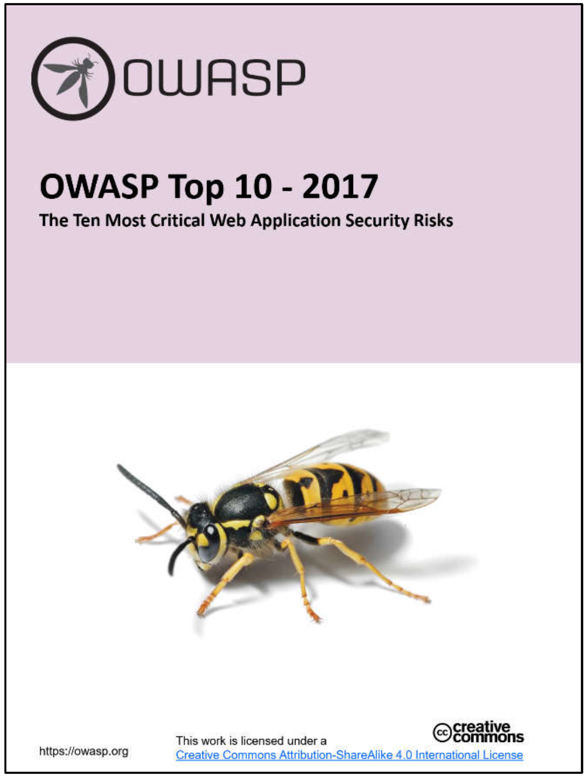
2017年

中国互联网
网络安全报告

国家计算机网络应急技术处理协调中心 著

CNCERT/CC
国家互联网应急中心

中国工信出版集团 人民邮电出版社
POSTS & TELECOM PRESS



OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

https://owasp.org

This work is licensed under a
Creative Commons Attribution-ShareAlike 4.0 International License

creative commons

Syllabus - Description

- **A. DESCRIPTION**
  - Prerequisite
    - ✧ Discrete Mathematics
    - ✧ C-like Languages
    - ✧ Operating Systems
    - ✧ Computer Networks

Syllabus - Organization

- **B. ORGANIZATION**
  - Lecture Time
  - Home works
  - Lab Works

Syllabus – Course Objectives

- **C. COURSE OBJECTIVES**
  - To introduce fundamentals of information security and applied technology
    - ✧ This course focuses on the fundamentals of information security that are used in protecting both the information present in computer storage as well as information traveling over computer networks. Interest in information security has been spurred by the pervasive use of computer-based applications such as information systems, databases, and the Internet. Information security has also emerged as a national goal in most countries with national defense and homeland security implications. Information security is enabled through securing data, computers, and networks.
    - ✧ In this course, we will look into such topics as fundamentals of information security, computer security technology and principles, access control mechanisms, cryptography algorithms, software security, physical security, and security management and risk assessment.

Syllabus – Course Objectives

- **C. COURSE OBJECTIVES**
  - Our works
    - ✧ Trusted Operating System – Analysis, design and implementation
    - ✧ Code Obfuscation – Code obfuscation for C source programs
    - ✧ Industrial Control Security – Secure stack design and implementation

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - Fundamentals of Information Security
    - ✧ Introduction to Information Security
    - ✧ Cryptographic Techniques
    - ✧ Authentication Techniques
  - Internet Security
    - ✧ Introduction to Internet Security
    - ✧ Network Attack and Defence
    - ✧ Firewall
    - ✧ Intrusion Detection & Protection
  - Web Security
    - ✧ The Architecture and Security of Web Applications
    - ✧ Security Flaws of Web Applications
    - ✧ Secure Web Programming
  - Lab Works

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - ✧ **Chap 1. Introduction to Information Security**
      - ◌ 1.1 Concept of Information Security
        - Situation of Information Security: Security situation report from CNCERT/CC
        - Definition of Information Security: security, information security, computer security and information assurance
        - History of Information Security
        - Key Concepts: CIA triad and others
      - ◌ 1.2 Computer System Security
        - Computer System Vulnerabilities
        - Operating System Security: components for OS security management
        - Database Security: concepts and components
        - User Application Security: concepts and components

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 1. Introduction to Information Security**
      - 1.3 Information Security Service
        - Basic Concepts
        - Authentication
        - Access Control
        - Confidentiality
        - Integrity
        - Availability
        - Non-repudiation
      - 1.4 Information Security Management, Audit and Protection
        - Security Management
        - Security Audit
        - Levels of Information Security: GB/T 20269-2006

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - ✧ **Chap 1. Introduction to Information Security**
      - 1.5 Conclusion
        - Standards Organizations
        - Computer Security Challenges
        - OSI Security Architecture: Series X
        - Attack Surface
        - Attack Trees
        - Security Service and Security Mechanism
        - Fundamental Security Design Principles
        - Balancing Information Security and Access
        - Information Security Implementation: bottom-up, top-down and dual-direction
        - The Security Systems Development Life Cycle

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 2. Cryptographic Techniques**
      - 2.1 Introduction
        - Definitions, *Kerckhoffs*' Principle, *Shannon*'s Maxim
        - History of Cryptology
        - Concepts & Items
        - Cryptosystems
        - Management of Cipher Keys
      - 2.2 Symmetric Key Cryptographic Algorithms
        - Introduction
        - Types & Modes: stream and block cipher, ECB, CBC, CFB, OFB
        - Data Encryption Standard (DES): DES algorithm in detail
        - Advanced Encryption Standard (AES): AES algorithm in brief

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 2. Cryptographic Techniques**
      - 2.3 Mathematical Foundations of Public-Key Crypto
        - Prime factorizations of integers
        - The *Euclidean* Algorithm
        - *Bézout*'s Theorem
        - Linear Congruence
        - The Extended_*Euclidean* Algorithm
        - The Chinese Remainder Theorem
        - *Euler*'s φ function
        - *Euler*'s Theorem
        - *Fermat*'s Little Theorem
        - Primitive Root & Discrete Logarithm

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 2. Cryptographic Techniques**
      - 2.4 Asymmetric Key Cryptographic Algorithms
        - Introduction: asymmetric key cryptographic requirements, Knapsack Problem, *Diffie-Hellman* key exchange algorithm
        - The RSA Algorithm: history, principles, *Miller-Rabin* algorithm
        - Examples of RSA applications: data confidentiality, authentication, digital signatures
      - 2.5 MAC and Hashing Algorithms
        - Message Authentication Code
        - Hash Function
        - Message-Digest Algorithm: MD5 in detail, SHA and RIPEMD in brief, HMAC
      - 2.6 Typical Applications

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 3. Authentication Technologies**
      - 3.1 Overview
        - Introduction to Authentication Technologies
        - The Weak/Strong Authentication Scheme: challenge-response with password, zero-knowledge proof, *Fiat-Shamir* algorithm
        - The Application of Authentication Technologies: X.509 and Kerberos
        - The Attack to Authentication: impersonation, replay, forced delay, interleaving, Oracle session and parallel session attacks
        - The Security Guidelines to Protect Authentication Schemes: risk mitigation strategy

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 3. Authentication Technologies**
      - 3.2 Public Key Infrastructure
        - Introduction to PKI
        - PKIX: components of PKIX
        - The Management of PKIX
        - Public Key Certificate
        - Trust Hierarchy Model
      - 3.3 Kerberos
        - History & Development
        - *Needham-Schroeder* Symmetric Key Protocol
        - Description of Kerberos
        - Kerberos Process in Detail
        - Drawbacks & Limitations

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module I. Fundamentals of Information Security**
    - **Chap 3. Authentication Technologies**
      - 3.4 X.509
        - History and Version
        - Certificate: structure of a X.509 certificate
        - Certification Authority
        - Distribution, Transportation and Revocation of Certificates
        - Security Problems
        - Applications

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 4. Introduction to Internet Security**
      - 4.1 Network Security Architectures
        - Network Security Architectures: physical, system, network, applications and management securities
        - Concepts of Information Security Model
        - Secure Operating System
        - Security Evaluation Criteria: TCSEC, ITSEC, BS 7799, CC (ISO/IEC 15408)
        - PDR, P2DR and PDRR Models
        - Information Assurance System: risk analyze, protect, detect, test and evaluate, react, restore, implement
        - IATF, Information Assurance Technical Framework: people, technology and operation; defense in depth

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 4. Introduction to Internet Security**
      - 4.1 Network Security Architectures
        - OSI/ISO 7498-2 Model: architecture
        - OSI Security Services and Mechanisms in Detail
      - 4.2 IPSec
        - Introduction: properties of IPsec
        - AH and ESP Protocols
        - Tunnel and Transport Modes
        - Concepts & Items: SA, SAD, SPI, SPD, IKE, HMAC
        - ESP protocol: encryption and decryption in tunnel mode and transport mode in detail
        - AH protocol: encryption and decryption in tunnel mode and transport mode in brief
        - IKE - Key Management of IPSec

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 4. Introduction to Internet Security**
      - 4.3 SSL/TLS
        - Security in the Transport Layer
        - A Simplified Picture of SSL
        - Basic Concepts: session, connection, write/read states, cipher suites, pre-master secret, Record Layer protocol, Handshake protocol, ChangeCipherSpec protocol, Alert protocol, Application Data protocol
        - TLS Handshake and Resume
        - Generating of Keys: applying PRF (RFC 5246) to generate keys from PMS
      - 4.4 VPN
        - Introduction to IPsec VPN
        - OpenVPN

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 5. Network Attack and Defence**
      - 5.1 Overview
        - Network Security Crisis: cyberspace and cybersecurity; virus, worm and Trojan; cyberspace ecology deterioration
        - Hacking & Hackers: activities of hacking
        - Network Threats: internal threats, unstructured external threats and structured external threat
        - Steps of Network Attack
        - Methods of Network Defense

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 5. Network Attack and Defence**
      - 5.2 Network Attacks
        - Consequences of Cyberattacks
        - Types of Network Attack: Eavesdropping, Data Modification, Identity Spoofing (IP Address Spoofing), Password-Based Attacks, Denial-of-Service Attack (DoS), Man-in-the-Middle Attack (MITM), Brute Force Attack, Compromised-Key Attack (盗取密钥攻击), Sniffer Attack, Application-Layer Attack
        - Port Scan: NMap & SuperScan; TCP scanning, SYN scanning, UDP scanning, ACK scanning, FIN scanning
        - Process of Idle Scanning

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 5. Network Attack and Defence**
      - 5.3 Password Cracking
        - The Vulnerability of Passwords
        - Password Selection Strategies
        - Password Cracking
        - Useful Tools: top 10
      - 5.4 Buffer Overflow
        - Background: process virtual memory, 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

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 5. Network Attack and Defence**
      - 5.5 Spoofing Attack
        - ARP Cache Poisoning
        - DNS Spoofing
        - Web Spoofing
        - IP Spoofing: Mitnick attack

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 6. Firewall**
      - 6.1 Introduction
        - Definition and Classification of Firewalls
        - Functions & Deployment of a Firewall
      - 6.2 Packet Filtering Firewall
        - What is Packet Filtering Firewall
        - How Packet Filtering Firewall Works
        - Advantages & Disadvantages
        - Attacking Packet Filtering Firewall
      - 6.3 Stateful Inspection Firewall
        - What is Stateful Inspection Firewall
        - How Stateful Inspection Firewall Works
        - Advantages & Disadvantages
        - Attacking Stateful Inspection Firewall

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 6. Firewall**
      - 6.4 Application Proxy Firewall
        - What is Proxy
        - Topological Graph of Proxy
        - Functions Offered by Proxy
        - Advantages & Disadvantage
        - Attacking Proxy
      - 6.5 Bastion Host
        - Topological Graph of Bastion Host
        - Design Principles of Bastion Host
        - Types of Bastion Host
        - Deployment of Bastion Host
      - 6.6 Iptables

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module II. Internet Security**
    - **Chap 7. Intrusion Detection**
      - 7.1 Introduction to IDS
        - Concept of Intrusion Detection
        - Methods of Intrusion Detection
      - 7.2 Framework of IDS
        - Basic Structure of IDS
        - Host-Based IDS (HIDS)
        - Network-Based IDS (NIDS)
        - HIDS vs. NIDS
      - 7.3 Introduction to IPS
        - The Need of IPS
        - Security Capabilities
        - Types of IPS
        - IPS vs. IDS

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module III. Web Security**
    - **Chap 8. The Architecture and Security of Web Applications**
      - 8.1 Overview
        - C/S and B/S Models
        - Web Site Architecture: hardware, 3-tiers software, MVC
        - Electronic Commerce Architecture
        - Apache & IIS Web Server: Netcraft web server survey
      - 8.2 Web Security Primer
        - Web Security – Beginning: why not secure, Web Security Technology, Web Security Flaws
        - Web Server Vulnerabilities
        - Web Services Secure Model: web service, SOA, Oracle’s SOA, SOAP, WS-Security
    - **Chap.9 Security Flaws of Web Applications**
      - 9.1 OWASP’s Top Ten Critical Web Application Security Risks

Syllabus – Course Outline

- **D. COURSE OUTLINE**
  - **Module III. Lab Works**
    - ✧ Lab 1. Network Mapper
    - ✧ Lab 2. ARP Spoofing
    - ✧ Lab 3. Windows Firewall
    - ✧ Lab 4. FTP Protocol Analysis

Syllabus - Resources

- **E. COURSE RESOURCES**
  - Course Notes
    - ✧ courseware_ns_sysu@163.com
  - References
    - ✧ *William Stallings, Lawrie Brown*. Computer Security. Pearson (2008)
    - ✧ *Ross Anderson*. Security Engineering, 2th ed. Wiley (2008)
    - ✧ *Eric Cole*. Network Security Bible, 2th ed. Wiley (2009)
    - ✧ *Dafydd Stuttard, Marcus Pinto*. The Web Application: Hacker's Handbook, 2th ed. Wiley (2011)
    - ✧ *Paco Hope, Ben Waltber*. Web Security Testing Cookbook. O'Reilly (2009)
  - Other Resources
    - ✧ ACM Digital Library
    - ✧ IEEE Computer Society Digital Library
    - ✧ Wiki
    - ✧ … …

Syllabus - Grading

- **F. GRADING PLAN**
  - Class Attendance & Performance 10%
  - Assignments 30%
    - Pls. send to TAs
      - S/N 1-60:
      - S/N 61-120:
      - S/N 121-180:
    - You can discuss the problems with your classmates, but all work handed in should be original, written by you in your own words and uploaded on time.
    - No late homework will be accepted.
  - Final Exam 60%

Syllabus – Classroom Rules

- **G. CLASSROOM RULES OF CONDUCT**
  - Cell phone using
  - Laptop using
  - Food & drink
  - Being Late for class