Microsoft

CISSP Training Kit

David R. Miller

Published with the authorization of Microsoft Corporation by:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, California 95472

ISBN: 978-0-7356-5782-3

1 2 3 4 5 6 7 8 9 QG 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Acquisitions Editors: Ken Jones and Michael Bolinger

Developmental Editor: Box Twelve Communications

Production Editor: Kristen Brown

Editorial Production: Online Training Solutions, Inc.

Technical Reviewer: Michael Gregg

Copyeditor: Kerin Forsyth

Indexer: Bob Pfahler

Cover Design: Twist Creative • Seattle

Cover Composition: Ellie Volckhausen

Illustrator: Rebecca Demarest

APPENDIX B

CISSP 60-minute review

Take this with you to the exam center.

Before entering the exam center, review these terms and mentally recall the definitions and related concepts. This will help you develop the mental big picture of CISSP just before the exam.

Spend approximately 1 to 2 minutes per page reviewing the following terms.

Chapter 1: Information security governance and risk management

Security objectives and controls

- CISSP Common Body of Knowledge (CBK)
- Human safety
- Valuable information assets
- CIA
  - Confidentiality
  - Integrity
  - Availability
- Loss/compromise
- Vulnerability
- Threat
- Threat agent
- Threat and matching vulnerability create risk
- Risk
- Level of risk is calculated from likelihood and impact
- Exposure/attack surface
- Compromise/exploit
- Countermeasure/control
- Litigation

- Due diligence
- Due care
- Prudent person rule
- Proximate causation
- Negligence
- Liability
- Security through obscurity
- Administrative controls
- Technical/logical controls
- Physical controls
- Layers of security
- Operational goals
- Tactical goals
- Strategic goals

Policies and frameworks

- Management from the top
- Drivers of the security framework
  - Risks associated with the specific industry/business
  - Applicable legal and regulatory compliance requirements
  - Senior management vision, posture, and ethics
- Organizational policies
  - Policies
  - Standards
  - Procedures
  - Guidelines
  - Baselines
  - Issue-specific
  - System-specific
- Information life cycle
  - Creation
  - Distribution
  - Use
  - Maintenance
  - Disposal

- Data classification
  - Data owner
  - Information asset inventory
  - Classification (valuation)
  - Classification criteria
  - Protective controls
  - Data/media labeling
  - Government classifications
  - Commercial classifications
  - Data protection based on classification
  - Access controls
  - Encryption
  - Data at rest
  - Data in transit
  - Data in use
  - Data expiration
  - Retention period
  - Declassification
  - Secure disposal
- Governance of third parties that have access to sensitive data

Risk management

- Acceptable level of risk/risk tolerance
- Risk analysis
- Risk assessment team
  - Asset inventory
  - Tangible/intangible assets
  - Reputation as an asset
  - Asset valuation
    - Quantitative analysis
    - Qualitative analysis
    - Delphi method
  - Asset classification
  - Threat modeling/threats to assets
  - Exposure factor (EF)

        - Single loss expectancy (SLE)
        - SLE = asset value x EF
        - Potential loss
        - Delayed loss
        - Annualized rate of occurrence (ARO)
        - Annualized loss expectancy (ALE)
        - ALE = SLE x ARO
        - Countermeasures
            - Mitigate vulnerabilities
            - Mitigate likelihood
            - Mitigate impact
        - Cost of a countermeasure
        - Control gap as a percent of the asset value
        - Residual risk = asset value x control gap
    - Cost effective countermeasures compared against ALE
    - Managing risk
        - Mitigate risk
        - Transfer risk
        - Avoid risk
        - Accept risk
    - Uncertainty analysis/assumptions

Security program

- Approved by senior management
- Documented within security policies
- Budget defined from risk analysis/ALE
- Organizational structure
    - Production
    - Security
    - Auditing
- Hiring practices
    - Verification of information provided
    - Screening/background check
    - Acceptable use policy
    - Monitoring policy
    - Nondisclosure agreement (NDA)

- Security training for all employees at time of hire and at least annually
- Security awareness through constant reminders, enforcement, regular training
- Supplemental security awareness training for privileged users
- Remedial security awareness training for violations
- Termination practices
  - Removal of all access, internal and external
  - Exit interview
  - Return of company assets
  - Reinforce agreements
- Management of third-party vendors, consultants, contractors
- Consistent policy enforcement
- Monitoring/auditing/assessment practices
- Ongoing metrics

Chapter 2: Access control

Control characteristics

- Control types: Major category (review from Chapter 1)
  - Administrative
  - Technical/logical
  - Physical
- Control types: Subcategory
  - Deterrent
  - Preventive
  - Detective
  - Corrective
  - Recovery
  - Compensative/complementary
  - Directive
- Combinations of major and subcategories of controls
- Threat modeling
- Controls mitigate vulnerability, likelihood, and impact, driven by threat

- Trusted path
  - Subjects use computers and programs to access objects
  - Subject: Active entity, person, or process
  - Object: Information asset
  - Access: Information flow, has direction

Authentication, authorization, and auditing

- AAA (Authentication, authorization, auditing—or Accounting from old dial-up servers)
  - Identification (claim)
  - Claimant/supplicant
  - Authentication (verification)
  - Authenticator
  - Zero-knowledge proof
  - Multifactor authentication
  - Mutual authentication
- Something you know
  - Personal identification number (PIN)
  - Password
  - Passphrase/virtual password
  - Cognitive passwords
  - One-time passwords
  - Password generator
  - Strong password: Length, complexity, maximum age, reuse, dictionary words
  - Password secrecy: Storage, sharing
  - Dictionary attack
  - Brute-force attack
  - Hybrid attack
  - Social engineering
- Something you have
  - Token device
  - Synchronous
  - Asynchronous
  - Challenge handshake
  - Memory card/swipe card
  - Smart card

        - Contact memory/smart card
        - Contactless memory/smart card
        - Transponder
        - Combi-card: One CPU (weaker); contact + contactless
        - Hybrid card: Two CPUs (stronger); contact + contactless
    - Something you are
        - Biometrics
        - Finger scan
        - Finger print
        - Palm print
        - Hand geometry
        - Hand topology
        - Iris scan
        - Retina scan
        - Voice print
        - Signature dynamics
        - Keystroke dynamics
        - False rejection rate (FRR): Type I Error
        - False acceptance rate (FAR): Type II Error
        - Crossover error rate (CER)
    - Single-sign-on technologies
        - Scripts
        - Kerberos
            - Key Distribution Center
            - Ticket Granting services
            - Ticket Granting Ticket
            - Tickets with expiration
            - Symmetric keys
        - Directory Services: Based on ITU-T/ISO X.500
            - LDAP
            - SESAME
            - Privileged attribute server
            - Privilege attribute certificate
            - Certificates
            - Asymmetric + symmetric keys

- Authorization
  - Authorization life cycle = Provisioning, review, revocation
  - Access privileges
  - Access controls
  - Privilege = Rights + permissions
  - Principle of least privilege
  - Authorization creep
- Mandatory access control
  - Lattice
  - Clearance
  - Classification
  - Need-to-know
  - Category
  - Government use
- Discretionary access control
  - Access control matrix
  - Access control list (ACL)
  - Capability
  - Commercial use
- Role-Based Access Control/Nondiscretionary
  - Security group
- Rule-Based Access Control
  - Firewall rules
  - Disk quotas
- Explicit permission: Assigned to user
- Implicit permission: Through group membership
- Inherited permission
- Decentralized access control
  - Workgroup, ad hoc
- Auditing
  - Audit logs
  - Central log repository (syslog)
  - Secure storage/archival
  - Real-time analysis
  - Security Information and Event Management (SIEM) system
  - Archival term often based on compliance requirements

- Integrity protection and validation of audit logs
- Scrubbing the logs
- Secure disposal

Remote access

- Centralized access control
  - Remote access control
  - AAA server
  - Authentication, authorization, accounting (or auditing)
  - RADIUS
  - TACACS
  - TACACS+
  - Diameter: Replacing RADIUS. Targeting 4G cellular networks

Intrusion detection and prevention systems

- Intrusion detection systems
  - Monitor, compare, alert
- Intrusion detection system response
- Intrusion prevention (protection) systems
  - Monitor, compare, alert and react
- Centralized IDS/IPS management/administrative console + sensors
- Signature and firmware updates
- Sensor connectivity (HW tap, span port, mirror port, diagnostic port)
- Sensor isolation (directed inbounds only from management server)
- Network-based IDS/IPS: Packets in the network only
- Host-based IDS/IPS: Processes within a system only
- Knowledge-based IDS/IPS
  - Only previously known attacks
  - Signatures/definitions/updates
- Behavior-based IDS/IPS
  - New attacks
  - Statistical
  - Anomaly
  - Clipping level
- False-positive
- False-negative
- Risks with using IPS: Self-imposed DoS

Chapter 3: Cryptography

History of cryptography

- Five cryptographic services
  - Confidentiality
  - Authentication
  - Nonrepudiation
  - Integrity protection and verification
  - Key distribution (secure)
- Data at rest
- Data in transit
- Data in use
- Cryptology
- Cryptography: Hiding and revealing messages
- Cryptanalysis: for good intent, for bad intent
- Three requirements for cryptography: Plaintext, key, algorithm
- Cipher/algorithm
- Key
- Encryption
- Plaintext
- Ciphertext
- Cleartext
- Key space
- Key clustering
- Cryptoperiod
- Work factor
- Moore's law
- Cryptosystem
- Strength of the cryptosystem
  - Strength versus performance
  - Governed by policy
  - Long, random, secret keys
  - Well-designed and implemented algorithms/ciphers into cryptosystems
  - Highly randomized ciphertext will not compress well

- Symmetric cryptography
  - Substitution cipher
  - Transposition cipher
  - Block ciphers
  - Substitution + transposition = 1 round
  - Stream ciphers
- Asymmetric cryptography
  - Diffie-Hellman (Merkle): 1976
  - Giant numbers + math
  - Calculating discrete logarithms in a finite field
- Hashing algorithm/message digest
  - Hashing process
  - Parity
  - CRC
  - MD family (Ron Rivest)
  - SHA family (SHA1, SHA2 from NIST)
  - HAVAL
  - RIPE
  - TIGER
  - Whirlpool
- Hashing: services provided
- Collision: Different messages + Same hash function = Same hash value
- Birthday attack
- Message Authentication Code: MAC/HMAC/CBC, MAC/CMAC
  - Hashes + symmetric key for authentication (weak) and integrity verification (weak)
- Hieroglyphics
- Atbash
- Scytale cipher
- Caesar cipher
- Mono-alphabetic cipher
- Vigenere cipher
- Poly-alphabetic cipher
- Kerchov's principle
- Gilbert Vernam—Stream cipher
- Vernam cipher—One-time pad

- Hebern rotor machine
- Enigma machine
- Diffie-Hellman asymmetric key algorithm
- Running key cipher
- Concealment cipher
- Steganography

Symmetric and asymmetric cryptography

- Symmetric key cryptography
- Secret, persistent, static, long-term keys
- Session, temporal, short-term keys
- Salt, seed, nonce, initialization vector
- Patterns in ciphertext
- George Boole: Boolean logic
- Binary
- Exclusive OR / XOR
- Truth table
- Block cipher
  - Software implementation: codes well
  - Key size
  - Block size
  - Substitution/confusion
  - Substitution Box/S Box/XOR
  - Transposition/diffusion
  - Rounds
  - DES/DEA/Lucifer
  - DES Cracker
  - 3DES
  - EEE3/EEE2/EDE3/EDE2
  - AES/Rijndael
  - IDEA
  - Twofish
  - Blowfish
  - RC5, RC6
- Ron Rivest

- Stream cipher
  - Approximately 1,000 times slower than block cipher
  - Hardware implementation: Linear feedback shift register
  - Key stream generator
  - RC4
- Symmetric key, block cipher modes
  - Electronic Code Book (ECB)
  - Cipher block chaining (CBC)
  - Output Feedback (OFB): Stream mode of any block cipher
  - Cipher Feedback (CFB): Stream mode of any block cipher
  - Counter (CTR): Stream mode of block cipher
- Symmetric key cryptography services provided
  - Confidentiality: Strong
  - Message Authentication Code (MAC)
    - Authentication: weak
    - Integrity verification (hash or CBC): weak
- Symmetric key management
  - Symmetric key, quantity of different keys: $N(N - 1)/2$
  - Symmetric key, # to protect: $N(N - 1)$
  - Key generation
  - Cryptographic service provider (CSP)
  - Out-of-band distribution
  - Secure key storage
  - Key archival/escrow
    - File-based
    - HSM
    - Key division
  - Key recovery
    - M of N
  - Key lifetime/cryptoperiod
  - Key destruction
- Symmetric key cipher strength vs. performance
- Asymmetric cryptography
  - Public key
  - Private key

- Diffie-Hellman (Merkle)
  - Key agreement protocol
  - Discrete logarithms in a finite field
  - Unauthenticated (MITM)
  - One cryptographic service provided: Secure key distribution
- Rivest Shamir Adleman (RSA)
  - Trap door
  - Factoring large number into its prime factors
  - Five cryptographic services provided
- El Gamal
  - Discrete logarithms in a finite field
  - Five cryptographic services provided
- Elliptical Curve Cryptosystem (ECC)
  - Discrete logarithms in a finite field of groups of numbers on elliptical curve
  - Five cryptographic services provided
- Knapsack, cracked twice
- Approximately 1,000 times slower than stream cipher

- Asymmetric key/Hybrid cryptographic services provided
  - Confidentiality: Strong
  - Authentication: Strong
  - Nonrepudiation: Strong
  - Integrity protection and verification: Strong
  - Secure key distribution: Strong
- Asymmetric key management
  - Asymmetric key, quantity of different keys: 2*N*
  - Asymmetric key # of keys to protect (private key only): *N*
  - Asymmetric key distribution
- Asymmetric key cipher strength vs. performance
- Comparison of symmetric vs. asymmetric cryptography

Hybrid cryptosystems

- Digital certificates
- Digital signature/Signing
  - Hashes + asymmetric key for authentication (strong) and integrity verification (strong)

- Signing: services provided
  - Authentication (Strong)
  - Non-repudiation (Strong)
  - Integrity validation (Strong)
- Signing process
- Verifying the digital signature
- DSS/DSA
- RSADSA/ECCDSA
- Data encryption/sealing
  - Sealing: Services provided

Confidentiality (Strong)

- Sealing process
- Key distribution
- PKI
  - Digital certificates
  - X.509v3
  - Digital certificate signed by CA
  - Digital certificate uses
    - Strong authentication
    - Nonrepudiation
    - Confidentiality
    - Integrity protection and verification
    - Signing messages
    - Signing software
    - Signing CA server certificates
    - Key distribution
  - Certification authority (CA)
  - Registration authority (RA)
  - Hierarchy of trust
  - CA hierarchy
  - Root CA
  - Subordinate CA
  - Policy CA
  - Issuing CA
  - Certificate practices statement (CPS)

- Revoking certificates
  - Certificate revocation list (CRL)
  - CRL distribution point (CDP)
  - Online Certificate Status Protocol (OCSP)
- PKI-enabled applications
- Trusted root CAs: Client systems
- Certificate repository
- Certificate verification
  - Trusted CA
  - Certificate details
  - CA signature verification
  - Revoked
- Cross certification
- Subordinated trust

- PGP
  - Commercial asymmetric cryptosystem
  - Web of trust
- Link encryption
- SSL
  - SSL process
- SSTP
- HTTP/S-HTTP/HTTPS
- SFTP/FTPS
- IPsec
- SSH
- S/MIME
- SET
- Attacks on cryptography
- Social engineering
- Attack on messages
- Attack on keys
- Brute force attack
- Rainbow tables
- Frequency analysis
- Birthday attack

- Replay attack
- Ciphertext-only attack
- Known plaintext attack
- Chosen plaintext attack
- Iterative/adaptive chosen plaintext attack
- Chosen ciphertext attack
- Iterative/adaptive chosen ciphertext attack
- Secure handling of keys

Chapter 4: Physical (environmental) security

Designing a secure facility

- First line of defense
- Safety is top priority
- Threats to physical security
  - Natural
  - Supply system
  - Human-made
  - Technical (loosely part of physical security)
- Liability aspect
- Part of security program
  - Defined by policies
- Goals of physical security countermeasures
  - Deter
  - Detect
  - Delay
  - Assess
  - Respond
- Crime Prevention through Environmental Design (CPTED)
- Perimeter security
- Location
- Construction
- Visibility/surveillance
- Entry and exit access control and logging

- Fire code
- Territorial reinforcement
- Data center location
- Emanations protection
  - Shielding
  - Faraday cage
  - Tempest
- Security zones
- Target hardening
- Full wall vs. partition
- Window design
- Door construction
- Positive air pressure
- Water detectors
- Locks
  - Conventional locks
  - Cipher locks
  - Pick resistant locks
  - Electronic locks/auditing
  - Key management
- Fences
  - Fences: 3–4 ft
  - Fences: 6–7 ft
  - Fences: 8+ ft
  - Fencing and gate considerations
  - PIDAS
  - Bollards
- Security guard advantages and disadvantages
  - Best physical security countermeasure: Deterrent, detective, preventive
  - Discriminating judgment/controlled response
  - Visitor control
  - Expensive
  - Background checks
- ID badges
- Piggybacking

- Turnstiles/mantrap/revolving door
- Fail safe
- Fail secure
- Guard dogs
- Signage: Directive, deterrent
- Lighting: Continuous
- Lighting: Motion triggered
- Lighting: Random
- CCTV cameras
  - Detection
  - Recognition
  - Identification
  - Field of view
  - Fixed/variable focus
  - Fixed/variable aperture
  - Monitoring station
- Securing portable devices
  - Cable lock
  - Strong authentication
  - Disk encryption
  - LoJack/phone home
  - Remote wipe
  - Awareness training
- Intrusion detection (physical)
  - Proximity
  - Acoustic/seismic
  - Doppler effect
  - Contact switch
  - Photoelectric
  - Pressure mat
- HVAC
  - Protect intake ducts
  - Humidity controls
  - Failure recovery

- Power
  - Secondary power feed
  - Power grid/substation
  - Generator
  - Line conditioner
  - Standby UPS
  - Online UPS
  - Static electricity
  - Spike
  - Surge
  - In-rush
  - Fault
  - Blackout
  - Brownout
  - Sag
  - EMI
  - RFI
  - Power strips, extension cords
- Shut off valves/switches
- Periodic walkthrough inspection
- Personnel monitoring
  - Insider threat
  - Safety
  - Stress, duress, disgruntled

Fire protection

- Four legs of a fire
  - Fuel
  - Heat
  - Oxygen
  - Chemical reaction
- Fire Detection
  - Ionization detector
    - Ion

- Thermal detector
  - Rate of rise
  - Fixed temperature
- Photoelectric detector
- Infrared detector
- Detector placement approximately everywhere

- 5 classes of fires
  - **Class A fire** Common combustibles
  - **Class B fire** Liquid fires
  - **Class C fire** Electrical fires
  - **Class D fire** Combustible metals
  - **Class K fire** Kitchen fires
- Fire extinguisher
  - Rating
  - Placement 50 feet from electrical equipment
  - Status/monitoring, inspect quarterly
- Fire suppression agents
  - Gas
  - Halon
  - Montreal Protocol
  - FM-200
  - CO2
  - Dry chemicals
  - Wet foam
  - Water
- Sprinklers
  - Wet pipe
  - Dry pipe
  - Pre-action system
  - Deluge system
- Fire plan and drill
  - Roles and responsibilities
  - Lessons learned

Chapter 5: Security architecture and design

Computer and operating systems

- CPU
- ALU
- Control unit
- Instruction
- Data
- Register memory
- Cache memory
- RAM
- ROM
- Data I/O
- Address bus
- Data bus
- Memory
  - Primary memory
  - Virtual memory: Hard disk
    - Swapfile/pagefile
    - Page in/page out/page fault
  - Memory manager
  - Physical addressing
  - Virtual addressing
  - Base address
  - Offset
  - Memory protection
  - Memory segmentation
  - Memory leak
- Multiprocessor
- Symmetric multiprocessing
- Asymmetric multiprocessing
- Trusted platform module (TPM)
- Application
- Process

- Process table
- Process states
  - Running
  - Ready
  - Blocked
- Buffer/stack
- Interrupts
- Thread
- Execution domains
  - User mode/problem mode/untrusted mode
  - Kernel mode/protected mode/trusted mode/supervisory mode
- Multiprogramming
- Multitasking: Cooperative
- Multitasking: Preemptive
- Multithreaded
- Security kernel
  - Local security authority (LSA)
  - Reference monitor
  - 3 rules for reference monitor
- Trusted recovery
  - Emergency system restart: Blue screen
  - System cold start: User initiated
  - Safe mode (single user mode)
- Security boundary
- Abstraction
- Multiplexing
- Layering
- Data hiding
- Encapsulation
- Segmentation
- Isolation
- Black box
- Deadlock
- Restricted/constrained interfaces
- Protection rings

- Process isolation
- Application programming interface (API)
- Device drivers
- Virtual machines
  - VMware
  - Hyper-V
  - Java Sandbox
  - Java Virtual Machine
  - VirtualBox
- System security modes: MAC
  - Dedicated security mode: Clearance = classification
  - System high-security mode: Clearance = classification, need to know = category
  - Compartmented security mode: Clearance = classification, need to know = category, permissions; lower classification data on system
  - Multilevel security mode: Clearance = classification, need to know = category, permissions; lower and higher classification data on system
- Cloud computing
  - Service-oriented architecture (SOA)
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Management concerns of third-party service providers
    - Risk analysis
    - Legal
    - Compliance
    - Service Level Agreements (SLAs)
- Grid computing: Multiple clouds working on common process

Security laws and frameworks

- Laws
  - HIPAA
  - Sarbanes-Oxley (SOX)
  - GLBA
  - FISMA
  - BASEL II
  - Others

- Industry Regulations
  - PCI: 12 major categories
- Frameworks/standards/best practice/vendor recommendations
- Frameworks
  - COSO: Enterprise framework for governance
    - CobiT: Control Objectives for IT, subset of COSO
  - Zachman Model: Enterprise architecture, management framework
    - SABSA model: Sherwood Applied Business Security Architecture,
    - Security for the business and IT subset of Zachman model
  - ISO/IEC 27000 series on information security
  - 27001: Information Security Management System (ISMS) (from BS7799-2)
  - 27002: Information Security Standard Code of Practice (was ISO 17799 from BS7799-1)
  - 27003: Implementation of an ISMS
  - 27004: Measurement and Metrics for ISMS
  - 27005: Information Security Risk Management
  - 27006: Certification and Accreditation of ISMS
- IT governance

Security models

- Subject uses computers and applications to access objects
- Trusted Computing Base (TCB)
- Security perimeter
- Access control models
- State machine
- Information flow
- Noninterference
- Bell–LaPadula
  - Confidentiality
  - MAC
  - Simple security property
  - Star property
  - Strong star property

- Biba
  - Integrity
  - MAC
  - Simple integrity axiom
  - Star integrity axiom
  - Invocation property
  - Three goals of the Biba model
- Clark–Wilson
  - Integrity
  - Access triple
  - Active agents
  - Transformation procedures (TPs)
  - Constrained data items (CDIs)
  - Unconstrained data items (UDIs), less trusted
  - Integrity verification procedures (IVPs)
  - Separation of duties + job rotation
- Brewer–Nash/Chinese wall
  - Dynamically assembled ACLs
  - Conflict of interest
  - Context-sensitive
  - Before you touch any data set, you can touch any data set
  - After you touch any one data set, you cannot touch any other data set
- Graham–Denning
  - User account provisioning
- Harrison-Ruzzo-Ullman (HRU)
  - An extension of Graham–Denning; more complex
- Take-Grant protection model

Certification and accreditation

- Functionality
- Assurance
- Operational assurance
- Certification

- Accreditation
- TCSEC
  - Based on Bell–LaPadula
  - NCSC
  - Rainbow series
  - Orange Book: Computer
  - Red Book (TNI): Network
  - TCSEC ratings
    - **A1** Verified Protection
    - **B3** MAC: Security domains
    - **B2** MAC: Structured protection
    - **B1** MAC: Labeled security protection
    - **C2** DAC: Controlled access protection
    - **C1** DAC: Discretionary protection
    - **D** Minimal security
- ITSEC
  - ITSEC members
  - Based on Bell-LaPadula
  - ITSEC ratings
    - Functionality F1: F10
    - Effectiveness E: E6
    - F and E mapping to TCSEC
  - F10: High confidentiality and integrity over networks
  - F9: High confidentiality
  - F8: High integrity during communications
  - F7: High availability
  - F6: High integrity
  - E6+F5 = A1: Verified protection
  - E5+F5 = B3 MAC: Security domains
  - E4+F4 = B2 MAC: Structured protection
  - E3+F3 = B1 MAC: Labeled security protection
  - E2+F2 = C2 DAC: Controlled access protection
  - E1+F1 = C1 DAC: Discretionary protection
  - E0 D: Minimal security

- Common Criteria: ISO 15408
  - Driven by business needs
  - Protection profile
  - Target of evaluation
  - Security target
  - Packages
  - EAL7: Formally verified design and tested
  - EAL6: Semi-formally verified design and tested
  - EAL5: Semi-formally designed and tested
  - EAL4: Methodically designed, tested and checked
  - EAL3: Methodically tested and checked
  - EAL2: Structurally tested
  - EAL1: Functionally tested
  - EPL

Chapter 6: Legal, regulations, investigations, and compliance

Computer crimes and motivations

- Define computer crimes: Breach of laws and regulations (vs. breach of policy)
- Role of computer in the crime
  - Target
  - Tool
  - Incidentally involved
- Computer Criminals: Who, why, and how
  - Motive, opportunity, means
  - Script kiddie
  - Skilled hacker
  - Social engineer
  - Fun
  - Grudge
  - Money/business
  - Denial of service (DoS, DDoS)
  - Salami

- Data diddling
- Dumpster diving
- Difficulties in prosecution
  - Not reported: Damage to reputation
  - Evidence is complex, intangible, difficult to collect and present
  - Laws lagging crimes
  - Jurisdiction issues
  - Lack of investigative/forensic/legal skills

Laws regarding computer crime

- Privacy laws
  - Personally identifiable information (PII)
  - Data collection, analysis, access
  - SOX, HIPAA, GLBA, PCI
  - Privacy Act of 1974
  - Electronic Communications Privacy Act of 1986
  - Compliance
  - Auditing: Internal and external
  - Due diligence, due care, prudent person, proximate causation, negligence, liability
  - Downstream liabilities and upstream liabilities
  - Governance of third parties
    - Cloud computing
    - Outsourcing
    - Consultants
    - Vendors
    - Risk analysis
    - Legal
    - Compliance
    - Service Level Agreements
- Global legal considerations
  - European privacy principles
  - Trans-border information flow
  - Employee privacy issues
  - Burden of proof
  - Penalties

- Common (code or codified) legal system
  - Europe, S. America
  - 500 AD Justinian codifies laws of Rome
  - Rule-based (not precedence-based)
- Common legal system (precedence-based)
  - England, US
  - Criminal
  - Civil (tort)
  - Administrative, regulatory
  - Nature of crime
- Customary legal system
  - China, India, Native Americans
  - Personal conduct and patterns of behavior
- Religious legal system
  - Islam, Hindu, Jewish
  - Revealed by deity(ies)
  - Obligations to others
  - Responsibilities
  - Religious duties
- Combinations of legal systems

- Intellectual property
  - Trade secret
    - Protected
    - Developed internally
    - Competitive value
    - Proprietary
    - Critical for survival of company
    - No registration required
  - Copyright
    - Original works of authorship
    - Protects the expression if ideas, not the ideas themselves
    - Source code

- Trademark
  - Word, name, symbol, sound, shape, color
  - Recognized as the company, look and feel
- Patent
  - Invention
  - Protection for a specified period
  - Novel
  - Not obvious

Investigating computer crime

- Global effort to standardize computer crime laws, evidence, and prosecution
  - G8 subgroup on high-tech crime
  - Interpol
  - International Organization on Computer Evidence (IOCE)
  - GAISP/GASSP
- Fourth Amendment: Search and seizure
  - Law enforcement official
  - Police agent
  - Citizen
- Notifying law enforcement
  - Management's decision
  - Loss of control on investigation, public information
  - Evidence collection: Removal/quarantine/storage
  - Might be required by law: Illegal if not reported
- Evidence
  - Chain of custody
    - Fully documented collection, security, possession, protection, transportation, integrity protection and verification
    - Separation of duties

- Evidence life cycle
  - Protection of scene/preservation
  - Identification
  - Documentation: Pictures, written
  - Collection
  - Order of volatility
  - Labeling
  - Transportation
  - Storage
  - Analysis
  - Verification (integrity not tampered)
  - Presentation in court
  - Return to victim (appeals?)
- Admissibility
- Relevance
- Prove or disprove assertion
- Best evidence
- Hearsay
  - Printed
  - Exception if routine business activity
- Interview (info) vs. interrogation (evidence)
- Enticement vs. entrapment

- Incident response
  - Monitoring/detection
  - Procedures
  - Team
  - Contact list
  - Escalation process
  - Event
  - Incident
    - Detect: Know it is happening
    - Triage: Impact assessment
    - Investigation: Exploit assessment
    - Containment: Response
    - Analysis: Vulnerability and eradication assessment

        - Tracking: Attacker analysis/evidence collection/prosecution
        - Recovery: Back to normal
        - Reporting: Ongoing and the big picture
        - Prevention: Lessons learned
- Forensic investigations
    - IOCE
    - Verification crime has been committed
    - Management defines law enforcement involvement
    - Documentation of actions: Thorough
    - Photograph scene, evidence
    - Order of volatility
    - Forensic tool kit
        - Physical
        - Digital
    - Analysis
        - Logs
        - Communications
        - Disk imaging: Bit-level copy
            - MAC times
            - Free space/slack space
            - Hidden content/ partitions
            - Steganography
        - Reverse code analysis
        - Exploit review

Ethical issues

- Corporate ethics
    - Established in policies, practices, awareness training
    - Examples of rules to promote ethical behavior
- ISC2 Code of Ethics
    - Protect society, the commonwealth, and the infrastructure
    - Act honorably, honestly, justly, responsibly, and legally
    - Provide diligent and competent service to principals
    - Advance and protect the profession
- Computer Ethics Institute

- Internet Architecture Board
  - Unethical
    - Purposely seeking to gain unauthorized access to Internet resources
    - Disrupting the intended use of the Internet
    - Wasting resources (people, capacity, and computers) through purposeful actions
    - Destroying the integrity of computer-based information
    - Compromising the privacy of others
    - Involving negligence in the conduct of Internet-wide experiments

Chapter 7: Telecommunications and network security

The OSI Model

- Seven abstraction layers
  - 7. Application
  - 6. Presentation
  - 5. Session
  - 4. Transport
  - 3. Network
  - 2. Data link
  - 1. Physical
- Protocols at layers
- Devices at layers
- LLC
- MAC
- Saving a file to a remote network location: Flow through OSI Model
- Identify destination
- Data stream
- Name resolution
- Segment
- Header
- Packet/datagram

- Addressing and routing
- Source IP address
- Destination IP address
- Local subnet or remote
- Routing decision
- Default gateway
- Frame
- Source MAC address
- MAC address resolution: ARP
- Destination MAC address
- CRC
- Trailer
- Bits
- Signal modulation/encoding bits on the wire
- Hops
- CRC verification at hops
- TCP/IP model

Transmission media and technologies

- Network media
  - Impedance
  - Interference
  - Attenuation
  - Crosstalk
  - Emanations
  - Coax cable
    - Thinnet: 10Base2
    - Thicknet: 10Base5
    - Terminator
    - BNC
    - Voltage/electrons
    - Radio frequency waves

        - Twisted-pair cable
            - UTP
            - STP
            - Plenum
            - Voltage/electrons
        - Fiber optic cable
            - Repeater
            - Light pulses/photons
        - Wireless
            - Radio frequency waves
    - Modulation and encoding
        - Analog
        - Amplitude
        - Frequency
        - Phase shift
        - QAM
        - Digital
        - Bipolar signaling
        - Synchronous signaling
        - Asynchronous signaling
        - Baseband
        - Broadband
    - Topologies
        - Bus
        - Ring
        - Star
        - Mesh: Full, partial
        - Tree
        - Hybrid
    - Intranet
    - Extranet
    - Internet

- IEEE 802 standards
- Unicast
- Broadcast
- Multicast
- Anycast
- Simplex
- Half-duplex
- Full-duplex
- Circuit switched
- Multiplexing
  - TDM
  - FDM
  - WDM
- Packet switched
- Media access methods
- Collision
- Contentionless/deterministic
- Contention-oriented/nondeterministic
- Polling
- Token-passing bus
- Token-passing ring
- CSMA-CA
- CSMA-CD

Infrastructure systems

- Client/endpoint systems
  - Desktop/workstation
  - Laptop
  - Pad device
  - Handheld device
  - Bring your own device (BYOD)

- Endpoint protection
  - Patching
  - Antivirus/anti-spyware/updates
  - Hardened system
  - Minimum services, software, user accounts
  - Principle of least privilege
  - Personal firewall
  - Host-based IDS/IPS
  - Configuration management
  - Acceptable use policies
  - Awareness training
- Remote access/remote administration
  - Screen scraper
- Virtual desktop: Platform as a service (PaaS)
- Virtual applications: Software as a service (SaaS)

- Mainframe
  - Thin client
  - SDLC/HDLC
  - Initial program load (IPL)
  - Unscheduled IPL
- Repeater
- Hub/concentrator
- MAU/MSAU
- Bridge
  - Collision domain
  - Broadcast domain
- Switch
- Modem
- Wireless access point
- Router
  - Route Table
  - Static/dynamic routing

- Gateway
- Dial-in server
- VPN server
- Firewall
  - Generation 1 firewall: Packet filter
  - Generation 2 firewall: Proxy server
    - SOCKS proxy
    - Circuit-level proxy
    - Application-layer proxy
  - Generation 3 firewall: Stateful Inspection
  - Generation 4 firewall: Dynamic packet filtering
  - Generation 5 firewall: Kernel proxy
  - Multihomed firewall
  - Screening firewall
  - Screened host
  - Screened subnet
  - White list/black list
- Default deny rule
- Ingress filter
- Egress filter
- Other firewall rules
- Perimeter network (also known as DMZ)
- Security zones
- DHCP
  - DORA
  - DHCP snooping
- LMHOSTS file
- WINS
- Hosts file

- DNS
  - DNS hierarchy
  - DNS zones
  - Resource records
  - Split DNS
  - Forwarder
  - Root hints
  - Root server
  - Top-level server
  - Authoritative name server
  - SOA
  - Resolver cache
  - DNSSEC
  - BIND
- Authentication server
  - PAP
  - CHAP
  - MS-CHAPv2
  - EAP
- NAT/PAT
  - One-to-one
  - One-to-many
  - Port forwarding
- Bastion host/hardened system
  - Types of systems to make bastion host systems
  - Regular updates to firmware, operating system, and applications
  - AV/AS/updates
  - Host-based firewall
  - File integrity verification
  - Dedicated function
  - Minimum user accounts
  - Least privilege
  - Minimum software
  - Remove administration tool set

Protocols, protocols, and more protocols

- Ports
- Source port/destination port
- Well-known port numbers: 0–1,023
- Ephemeral port numbers: 49,152–65,535
- TCP/IP
  - TCP
    - High overhead
    - Three-way handshake
    - TCP flags
    - Connection oriented/guaranteed delivery
  - UDP
    - Low overhead
    - Connectionless/best-effort delivery
- IPv4
  - 32 bits/4 octets
  - IP addressing
  - Classful addresses
  - Subnetting/CIDR
  - Private IP addressing
  - Public IP addressing
  - Internet dark address space
- IPv6
  - 128 bits/4 hexadecimal characters per group/8 groups
  - :: = all zeros in between
- Telnet
- BootP
- DHCP
- FTP/TFTP/SFTP/FTPS
- ICMP
- ARP
  - ARP cache

- SNMP
  - SNMP manager/agent
  - Public community string
  - Private community string
  - Get/Get Next/Set/Trap
- SMTP
- POP3
- IMAP4
- HTTP/HTTPS
- LDP
- NFS
- DNS
- Dynamic routing protocols
  - RIP/RIPv2
  - IGRP/EIGRP
  - BGP
  - Distance vector
  - OSPF
  - Link state
  - Autonomous system (AS)
- QoS
- MPLS
- Encrypted channels/VPNs
  - SSH
  - L2F
  - PPTP
  - L2TP
  - SSL
  - SSTP
  - IPsec
    - Internet Key Exchange v2
    - ISAKMP
    - Oakley Key Exchange

        - IPsec Security Associations
        - IPsec AH
        - Integrity check value (ICV)
        - IPsec ESP
        - IPsec Transport mode/End-to-end
        - IPsec Tunnel mode
        - IPsec authentication
        - IPsec Security Parameter Index
    - Link encryption

PAN, LAN, MAN, WAN, and then some

- PAN
    - IEEE 802.15
    - Bluetooth
    - Piconet
    - Zigbee
- LAN
    - VLAN
- MAN
    - Cable modem
    - ADSL/SDSL
    - FDDI
    - CDDI
    - SONET
    - Optical Carrier: 52 MB
- WAN/GAN
    - ISDN
    - T1/E1
    - T3/E3
    - BRI/PRI
    - B Channel
    - D Channel
    - X.25

- Frame relay
  - PVC
  - SVC
  - CIR
- ATM
  - 53-byte cell
- Satellites
- PSTN/POTS
  - SLIP
  - PPP
- PBX
- VoIP
  - SIP/H.323
  - Real-time Transport Protocol (RTP)
  - Jitter
  - Latency
  - Media Gateway

Wireless networking

- Benefits of wireless
- IEEE 802.11
- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11i
- Other IEEE 802.11 specifications
- Ad hoc/peer-to-peer
- Infrastructure
- Wireless access point
- Spread spectrum
- FHSS
- DSSS
- OFDM
- MIMO

- 2.4GHz
- 5GHz
- Association
- Cell
- Channel
- FCC
- SSID
- SSID broadcast
- Roaming
- Signal strength
- Cell shaping
- WEP
- PSK/SKA
- Open authentication
- MAC filtering
- WPA personal
- WPA enterprise
- TKIP/MIC
- Robust Secure Network
- WPA2 personal
- WPA2 enterprise
- AES/CCMP
- IEEE 802.1x port-based authentication
- WiMAX
- Cellular
  - First generation: 1G
  - Second generation: 2G
  - Third generation: 3G
  - Fourth generation: 4G LTE (Pre-4G), 4G
    - Will use alternate MAC and PHY (AMP) = WiMAX
- FDMA/TDMA/CDMA/CDMA 2000
- GSM
- SIM card

Attacking the network

- Browsing attack
- Targeted attack
- DoS
  - SYN flood
  - Ping of death
  - Teardrop attack
  - Land attack
- DDoS
- Information theft
  - Eavesdropping/sniffing
  - Emanations detection
  - ARP cache poisoning
  - DNS poisoning
  - Route poisoning
  - MITM
  - Session hijacking
- Traffic analysis
  - Pad the traffic
- Backdoor, maintenance hook
- Instant messaging (IM)
- Wireless attacks
  - Rogue wireless AP
  - War driving/war chalking
  - Cracking WEP
  - Bluejacking
- Cell phone cloning
- Cell phone tumbling
- Cell phone networks connections bypass LAN security controls
- Cell phone storage
- Cell phone camera

- Cell phone audio recording
- Gap in the WAP
- Phone company slamming
- Phone company cramming
- PBX maintenance modem
- Toll fraud

Chapter 8: Business continuity and disaster recovery planning

BCP and DRP plans

- How DRP/BCP gets started
  - Human safety
  - Prudent management
  - Legal and regulatory compliance
  - Fiduciary responsibility
- Defined in policies
- Disaster recovery vs. business continuity
  - DRP
    - Subset of BCP
    - Short Term response to disaster
    - Stabilize the patient, stop the bleeding
    - Recover critical business functions
    - Usually IT focused
    - Reduce losses short term
  - BCP
    - Preventive actions ongoing
    - Long-term recovery to normal operations
    - Ensures long-term survivability of business
    - Reduce losses long term

- Components
  - Define need for DRP and BCP
  - Define scope, team, roles, schedule
  - Identify business functions, dependency functions, assets
  - Perform business impact analysis (BIA)
  - Identify preventive controls
  - Develop disaster recovery plan/strategy (DRP)
  - Develop BCP
  - Get approval/budget
  - Test plans
  - Maintain plans
- Manage like a business project
- DRP/BCP team

Business impact analysis

- Business impact analysis
  - Identify critical business functions and required assets/resources
  - Identify maximum tolerable downtime (MTD)
  - Identify vulnerabilities and threats to the critical functions, assets, and resources
  - Determine risk level (likelihood + impact)
  - Develop recovery strategies within MTD
- Data gathering: Identify critical business functions and required assets/resources
  - Dependencies
  - Human assets/critical personnel
  - Processes
  - Technologies
  - Data
  - Work space
- Identify maximum tolerable downtime (MTD) for each critical function: Fatalistic view
  - Shortest times are most critical first to be addressed
  - Critical/essential
  - Urgent
  - Important
  - Normal
  - Nonessential

- Identify vulnerabilities and threats to the critical functions, assets, and resources
  - Natural
  - Technical
  - Supply system
  - Human
- Determine risk level (likelihood + impact)
  - Consider compliance requirements

BC and DR solutions

- Identify preventive controls
- Develop recovery strategies within MTD
- Countermeasures target vulnerabilities, likelihood, impact, and recovery
- Balance cost of disruption with cost of recovery
- Business processes
  - Alternate procedures (in case one is gone)
- Facility/user environment
  - Redundant/alternate site
  - Alternate site location
  - Subscription services
    - Cold site
    - Warm site
    - Hot site
  - Rolling hot site
  - Reciprocal agreements
  - Collocation
  - Acquire before it is needed
  - Increased costs
  - Risks increase but same security/protections required
- Technology
  - Redundancy
  - Compatibility
  - IT infrastructure
  - Communications systems

- Data
  - Collocation
  - Backups
    - Practice restore in hot site
  - Tape vaulting
  - Synchronous replication: Real time
  - Asynchronous replication: Near real time or batch job
  - Remote journaling
  - Disk shadowing
  - Electronic vaulting
  - Clustering
- Personnel
  - Critical personnel
  - Injured or worse
  - Dealing with family
  - Executive succession planning
  - Training and cross-training
- Supply systems
  - Resources
  - HVAC
  - Raw materials
  - Vendors/customers

Developing the plan

- Developing the plan for each department/function
- Developing the plan for the entire organization
- Preventive measures
- Components of the plan
  - Roles and responsibilities
  - Activation of the plan
  - Recovery
  - Business continuity
  - Appendices

- Roles and responsibilities
  - Team coordinator
  - Public relations
  - Damage assessment team
  - Relocation team
  - Restoration team
  - Network recovery team
  - Security team
  - Salvage team
  - Telecom team
  - Plan maintenance
- Activation of the plan
  - Who can declare incident/disaster/catastrophe
  - Criteria
  - Evacuation/safety procedures
  - Call list
    - What information to provide to entities called
    - Emergency services
    - Management
    - Team members
    - Shareholders
    - Customers
    - Vendors
    - Media
  - Approved responses/procedures
  - Maintain security thresholds
- Recovery of critical business functions within MTD
  - Written procedures
  - Coordination/communications between teams
  - Business continuity
  - Return to normal operations
    - Least critical functions return to primary site first

        - Maintain security thresholds
        - Test and verify systems (certification and accreditation)
        - Termination of DRP/BCP activities
        - Lessons learned/feedback/improvement
    - Appendices
        - Contact list with phone numbers, type of info to provide
        - Assignments
        - Diagrams
        - Schematics
        - Maps
        - Vendors/suppliers
        - Alternate plans
    - Copies of plan distributed, tracked, and secured
    - Testing the plans
        - Checklist (unit testing)
        - Structured walkthrough (tabletop, integration testing)
        - Simulation
        - Parallel
        - Full interruption
    - Objective of testing
    - Training the team members/cross-training
    - Maintaining the plan
        - Feedback loop
        - Causes of plans needing update
            - New or discontinued functions
            - Changes in MTD: Criticality of business functions
            - Changes in facilities
            - Changes in technology: Hardware and software
            - Personnel turnover (team members, critical personnel, and so on)
        - Change control for the plans

Chapter 9: Software development security

Software development life cycle and change control

- Application development
  - Security permeates all phases
- Software development models
- SDLC
  - Security permeates every stage
  - Project initiation
  - Functional design
  - System design
  - Software development
  - Installation/test
  - Operational maintenance
  - Disposal/end of life
- Capability Maturity Model Integration
- Initiating, Diagnosing, Establishing, Acting, Learning (IDEAL)
- Testing
  - Unit testing
  - Integration testing
  - Acceptance testing
  - Regression testing
  - Programming vulnerabilities
    - Garbage collection
    - Maintenance hooks
    - Covert channels
  - Verification: Product meets design specifications
  - Validation: Product satisfies customer's needs
  - Operational assurance
  - Life cycle assurance
- Software escrow

- Change control
  - Formal request for change
  - Analyze request
  - Implementation strategy
  - Cost vs. benefit
  - Security implications
  - Submit for approval
  - Code changes
  - Document new code
  - Test new program
  - Change revision
  - Release to library
  - Complete documentation
- Separation of duties: Dev/QA/library/production
- Updating
  - Firmware
  - Operating system
  - Applications
  - Virus definitions
  - IDS signatures
  - Procedures
    - Actively search for new patches
    - Test/approval
    - Rollback procedures
    - Change control
    - Deploy
    - Document
  - Time-sensitive
- Logging
  - Know what you need vs. what you're getting
  - Archive for compliance
  - Secure and verify integrity
  - First copy: Isolate from administrators for trusted audit trail
  - Second copy: For administrator review

Programming concepts

- Development
  - Programming tools and platforms
  - Application communications
- CASE tools
- First generation language: Machine Language
- Second generation language: Assembly language, hexadecimal, assembler
- Third generation language: High-level language, scripts, compiler, interpreter
- Fourth generation language: Very high-level language
- Fifth generation language: Natural or spoken language (AI)
- Object-oriented programming
  - Procedural vs. object-oriented
  - Modularity
  - Deferred commitment
  - Reusability
  - Naturalness
  - Classes
    - Variables
    - Attributes
    - Programmed behaviors
  - Objects, instantiated from classes
    - Defined variables, attributes, and programmed behaviors
  - Method
  - Message
  - Object has APIs: Input constraints, abstraction, black-box methods
  - Polymorphism: Many versions of objects from same class, common controls
  - Cohesiveness: Self-contained, desired high
  - Coupling: Integration with other objects, desired low
- Distributed computing
  - COM, DCOM, OLE
    - Windows
  - ORB, CORBA
    - Platform independent
  - J2EE

- Active content
  - Client-side processing
  - ActiveX
    - Windows
    - COM
    - Authenticode
  - Java applets
    - Platform independent
    - Java Sandbox
    - Java VM
    - Bytecode

Database systems

- Database management systems
- Database models
  - Hierarchical
    - One parent
    - Flat
  - Network
    - Multiple parents
  - Object-oriented
    - Stores data, graphics, audio, video, and program instructions
    - No need for high-level programming language
  - Relational
    - Rows and columns
    - Cell
    - Data element = Atomic
    - Primary key
    - Attribute
    - Record = Tuple
    - Foreign key
    - Entity integrity
    - Referential integrity

- Object relational
  - Combine object-oriented and relational
- Accessing databases
  - ODBC
  - OLE
  - ADO
  - JDBC
  - XML
  - SAML
- Web applications
  - Web-based authentication
  - Open Web Application Security Project (OWASP)
- Transaction processing
  - Concurrency control
    - Record locking
- Commit
- Rollback
- Checkpoint protection
- Two-phase commit
- ACID
  - Atomicity
  - Consistency
  - Isolation
  - Durability
- Constrained views
- OLTP
- Database warehouse
  - Normalization
  - Sanitization
- Database Mart: Subset of warehouse
- Data mining
- Metadata

Artificial intelligence

- Artificial intelligence
- Knowledge management
  - Data + context = information
  - Info + meaning = knowledge
  - Knowledge + insight = wisdom
- Knowledge discovery
  - Probabilistic
  - Statistical
  - Classification
- Expert systems
  - Survey experts
  - If–then else rules
  - Inference engine
- Artificial Neural Network
  - Computers connected like human brain neurons
  - Can learn from scenarios

Attacks on applications

- Aggregation and inference
- Malware
  - Virus
  - Worm
  - Trojan horse
  - Rootkits
    - Kernel mode
    - User mode
  - Backdoors
    - Maintenance hooks
- Covert channels
  - Storage
  - Timing

- Timing attacks
  - Race condition
  - Time of check/time of use
- Traffic analysis: Padding
- Meme: Rumors, urban legend
- Detection mechanisms
  - Signature
  - Heuristic
  - Integrity validation
  - Behavior
- HTTP response splitting
- Cross-site scripting (XSS)
  - Persistent
  - Nonpersistent
  - DOM
- Web cache poisoning
- Browser cache poisoning
- Cross-user defacement attacks
- Hijacking pages
- Active email content
- SQL injection
- Sensitive data retrieval
  - Cookies
    - Session
    - Persistent
  - Browser cache
  - Server error: Too much information
- Directory transversal
- Buffer overflow

Chapter 10: Operations security

Activities of the operations department

- Provide availability and safety
- User provisioning
  - Creation/disable/delete
  - Least privilege
  - Authorization creep
- Fraud protection
  - Separation of duties
  - Job rotation
  - Mandatory vacations
  - Dual control
  - Auditing
  - Least privilege
  - Collusion
- Roles
  - Data owner
  - System owner
  - Data custodian
  - System custodian
- Configuration management
  - Documentation
  - Auditing
  - Change management
  - Configuration integrity verification
  - System repairs and updating
  - Remote administration
- Vulnerability assessment
  - Vulnerability scanning
  - Software/firmware bugs
  - Misconfiguration
  - Compliance
  - Eliminate single points of failure

        - Fault tolerance
        - Redundancy
    - Penetration testing
        - Pen test agreement
        - Pen test terms of engagement
        - Hold harmless clause
        - Pen test scope
        - Full disclosure: White box
        - Partial disclosure: Blind, gray box
        - No Disclosure: Double blind, black box
        - Point-in-time analysis
        - Personnel pen test: Social engineering
        - Physical pen test
        - System and network pen test
- Remediation
- Honey pots/Honey nets/padded cell
    - Enticement
    - Entrapment

Media management

- Data classification/declassification
- Media library
    - Librarian
    - Software licensing
    - Media labeling
- MTBF
- MTTR
- Single point of failure
- Redundancy
- RAID 0, 1, 2, 3, 4, 5, 10, 15
    - Disk duplexing
- RAIT
- MAID: Power reduction, longer life
- Direct access
- Sequential access

- SAN
- Redundant servers, server farm, clustering
- Service-level agreements
- Collocation
- Backup types
  - Full
  - Incremental
  - Differential
  - Archive bit
  - Restoring from backup
  - Practice/test restore
- Hierarchical storage management (HSM)
- Data retention requirements
- Secure deletion/destruction
- Object reuse
  - Data remanence
  - Degaussing
  - Zeroization
  - Wiping/overwriting
- Fax security
  - Common output bin
  - Fax encrypter
  - Fax server
  - Fax to email mailbox

Attacks on operations

- Password cracking
- Key cracking
- Emanations detection
- Social engineering
- Dumpster diving
- Keyboard loggers
- Hacking: Black hat
- Penetration Testing: White hat

- Random/browsing/spray and pray attack
- Targeted attack
- Malicious code
- Zero-day attack
- Denial of service (DoS)
- Distributed denial of service (DDoS)
- Advanced persistent threat (APT)
- Passive reconnaissance
  - Sniffer
  - Protocol analyzer
  - Public information
  - Web searches
- Active reconnaissance
  - Scanning
  - Probing
  - Footprinting
    - Network scanning
    - War dialing
    - War driving
  - Fingerprinting
    - System/device type
    - Operating system
    - Applications/services/listeners
    - Versions
    - Update levels
  - Vulnerability database
- Exploit
  - Exploits: Attack code
- Escalate privilege
  - Exploit other services
  - Crack shadow file: Passwords
  - Access cached credentials: Passwords
  - Copy SAM file: Rainbow tables

- Entrench
  - Malware
  - Trojan
  - Backdoor
  - Rootkit
  - Harden system
  - Disallow AV/AS/IDS updates
  - Modify hosts file/redirect DNS
- Cover tracks
  - Scrub the logs
  - Hidden partition, files, and so on
  - Modify administrative reports
- Pillage
- Pivot and attack