The hyperlinks contained within this document are functional only when students are logged into the classroom. All topics are required reading unless indicated as recommended. Recommended items add additional context and knowledge related to the topics and projects, but not essential for completing the projects in the class.

CST620 Reading and Resource List

Project 1

Project 1 Step 1

Authentication

1. NIST Special Publication 800-57 Part 1, Revision 3
2. How to Authenticate Users with API Keys
3. Key Management Cheat Sheet
4. User Authentication with OAuth 2.0
5. Centralized Authentication Using OpenLDAP
6. Message Authentication Codes
7. Has The Time Come to Kill the Password?
8. Towards Secure and Dependable Message Authentication in WSN Recommended
9. Message Authentication and Source Privacy in Wireless Networks Recommended
10. Biometrics Recommended
11. Security How-To: WPA2-Enterprise on Your Home Network Recommended
12. Production Best Practices: Security Recommended
13. Protecting Your System: User Access Security Recommended
14. Authentication Recommended
15. Top 10 2013-A2-Broken Authentication and Session Management Recommended
16. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
17. Activity: Message Authentication Recommended
18. Authentication Summary Recommended
19. Multifactor Authentication Overview Recommended
20. Authentication and Information Assurance Recommended
21. Check Your Knowledge (Test)

Data at Rest

1. NIST Assessment Cases- System and Communications Protection- Protection of Data at Rest

Data in Motion

Insecure Handling

1. WASC Threat Classification
2. Insecure Cryptographic Storage
3. Cyber Security Course: 19 Data in Transit. Learn Internet Security
4. Guide to Malware Incident Prevention and Handling for Desktops and Laptops
5. A Report on the Privilege (Access) Management Workshop
6. OWASP Backend Security
7. Industry Draft: NIST SP 800-118: Guide to Enterprise Password Management
8. Guide to Storage Encryption Technologies for End User Devices
9. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
10. Data Backup Options Recommended
11. NIST Assessment Cases- System and Communications Protection- Protection of Data at Rest Recommended

Project 1 Step 3

Crypto Attacks

1. Cyber Attacks Explained: Cryptographic Attacks
2. Shannon's Maxim
3. Kerckhoffs's principle (Equivalent to Shannon's Maxim)
4. Blind Birthday Attack
5. Enhanced Cryptography by Multiple Chaotic Dynamics
6. Encryption - CBC Mode IV: Secret or Not?
7. Chosen Ciphertext Attacks
8. XOR Known-Plaintext Attack
9. Known Plaintext
10. Chosen Plaintext
11. Vulnerability to Attack
12. Check Your Knowledge (Test)

Project 1 Step 4

Uses of Encryption

1. Full-Disk Encryption
2. Data Encryption
3. Full Disk Encryption on Linux
4. How To Use DM-Crypt to Create an Encrypted Volume on an Ubuntu VPS
5. Volume Encryption Supported by the Key Manager

6. Data Encryption and Decryption by Using TripleDES and Performance Analysis of Crypto System

Hash Functions

1. Hash Functions
2. The Hashing Process

Types of Encryption

1. Symmetric Encryption Introduction
2. Asymmetric Encryption
3. Cryptographic Systems

DES

Triple DES

1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

Authentication (Repeated for Convenience)

1. NIST Special Publication 800-57 Part 1, Revision 3
2. How to Authenticate Users with API Keys
3. Key Management Cheat Sheet
4. User Authentication with OAuth 2.0
5. Centralized Authentication Using OpenLDAP
6. Message Authentication Codes
7. Has The Time Come to Kill the Password?
8. Towards Secure and Dependable Message Authentication in WSN Recommended
9. Message Authentication and Source Privacy in Wireless Networks Recommended
10. Biometrics Recommended
11. Security How-To: WPA2-Enterprise on Your Home Network Recommended
12. Production Best Practices: Security Recommended
13. Protecting Your System: User Access Security Recommended
14. Authentication Recommended
15. Top 10 2013-A2-Broken Authentication and Session Management Recommended
16. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
17. Activity: Message Authentication Recommended
18. Authentication Summary Recommended
19. Multifactor Authentication Overview Recommended
20. Authentication and Information Assurance Recommended
21. Check Your Knowledge (Test)

Cryptanalysis

1. Cryptography
2. Understanding Cryptology:Cryptanalysis

3. Trial Encoding Algorithims Ensemble
4. Improved Differential-Linear Cryptanalysis of 7-Round Chaskey with Partitioning

Public Key Infrastructure

1. Public Key Infrastructure
2. How Public Key Cryptography (PKC) Works
3. OpenVPN: Extended Verification of X.509 Client Certificates
4. Quantum Key Management
5. Check Your Knowledge (Test)

x.509

Project 1 Step 5

Ciphers

1. Unit 3: Block Ciphers
2. Design and Implementation of a Secure Stream Cipher for Cryptographic Applications
3. Chapter 6 Stream Ciphers
4. Classical Cryptography
5. New Secure and Advanced Algorithm for StreamCiphers Extended RC4 and FPGA Implementation
6. Encrypting Using XOR and a Password
7. Attacks on Stream Ciphers
8. Two-Key Dependent Permutation for Use in Symmetric Cryptographic System
9. Cipher Scheme Hybrid Additive Cellular Automata
10. RC4 Stream Cipher and Possible Attacks on WEP
11. Transposition and Substitution in Ciphers
12. Caesar Shift Cipher
13. Cryptographic Systems
14. Block vs. Stream Ciphers

Project 1 Step 7

Digital Certificates

1. Certificate Authorities API - User Guide
2. Digital Signatures and Certificates
3. A Model of Certificate Revocation
4. Lecture 14: SSL and HTTPS

Project 2

Project 2 Step 1

Wireshark

User Datagram Protocol (UDP)

Transmission Control Protocol/Internet Protocol (TCP/IP)

1. Base of the Networking Protocol: TCP/IP Its Design and Security Aspects
2. Haktip 3: Packet Sniffing 101: Promiscuous Mode
3. TCP/IP: The Internet's Secret Sauce Recommended
4. TCP / IP Suite Recommended
5. Securing Computer Systems: TCP/IP Security Recommended

Internet Packets

IP Address Schemes

1. How To Isolate Servers Within A Private Network Using Iptables
2. Representing Data
3. Comparison Between Traditional IPNetworks/Routing and MPLs
4. Math Operations

Well-Known Ports and Applications

1. Check Your Knowledge

Intrusion Detection & Prevention (IDS/IPS) Systems

1. Intrusion Detection Systems (IDS) by Marr Madden
2. Intrusion Detection Systems (IDS)
3. Intrusion Detection
4. False Positive Responses Optimization for Intrusion Detection System
5. A Model for Anomaly Classification in Intrusion Detection Systems

Firewalls (Repeated for Convenience)

1. Technological Safeguards
2. Types of Firewalls
3. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices
4. What is a Firewall and How Does It Work? Recommended
5. Deep Packet Inspection Based on Many-Core Platform Recommended
6. Iptables Essentials: Common Firewall Rules and Commands Recommended
7. Creating Firewall Rules Recommended
8. Network Address Translation Reference Recommended
9. Guidelines on Firewalls and Firewall Policy Recommended

Project 2 Step 2

Cyberattacks (Repeated for Convenience)

1. A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD
2. Collusion-Tolerable and Efficient Privacy-Preserving Time-Series Data Aggregation Protocol Recommended

3. Collusion-Resistant Audio Fingerprinting System in the Modulated Complex Lapped Transform Domain Recommended
4. Covert Encryption and Document Authentication Using Texture Coding Recommended
5. SQL Injection Prevention Cheat Sheet
6. Cache Poisoning
7. Robust Image Watermarking Theories and Techniques: A Review Recommended
8. OWASP Periodic Table of Vulnerabilities - Cookie Theft/Session Hijacking Recommended
9. Spoofing Attacks on Packets and Methods For Detection and Prevention of Spoofed Packets
10. Detection and Modeling of Cyber Attacks with Petri Nets
11. A Copyright Protection Scheme for Digital Images Based on Shuffled Singular Value Decomposition and Visual Cryptography Recommended
12. Dual Watermarking For High Protective Copyright System
13. DDoS Quick Guide Recommended
14. DRAFT Guide to Cyber Threat Information Sharing Recommended
15. Insecure Randomness Recommended
16. Digital Watermarking Recommended
17. Cyber Attacks Explained: Cryptographic Attacks
18. Testing for Padding Oracle Recommended
19. Stochastic Image Warping for Improved Watermark Desynchronization Recommended
20. Video Multiple Watermarking Technique Based on Image Interlacing Using DWT Recommended

Spoofing/Cache Poisoning Attacks (Repeated for Convenience)

1. Cyber Attacks Explained: Cryptographic Attacks
2. Cache Poisoning
3. Spoofing Attacks on Packets and Methods For Detection and Prevention of Spoofed Packets
4. Spoofing/Cache Poisoning Attacks Recommended

Man-in-The-Middle Attacks

Honeypots

Project 2 Step 3

False Positives and False Negatives

Project 2 Step 5

Intrusion Detection & Prevention (IDS/IPS) Systems (Repeated for Convenience)

1. Intrusion Detection Systems (IDS) by Marr Madden

2. Intrusion Detection Systems (IDS)
3. Intrusion Detection
4. False Positive Responses Optimization for Intrusion Detection System
5. A Model for Anomaly Classification in Intrusion Detection Systems

Network Forensics Analysis

1. Check Your Knowledge (Test)

Project 3

Project 3 Step 1

Network Security Threats

Threat Modeling

Mobile Architectures

Application Security

Operating System Security

1. System and Kernel Security
2. How To Use the Linux Auditing System on CentOS 7
3. Ring (Computer Security)
4. Operating Systems Security: Protection Measures Analysis
5. A Security Adaptation Reference Monitor for Wireless Sensor Network
6. Security: An Advanced Introduction
7. Error Handling, Auditing, and Logging
8. Using Proven Reference Monitor Patterns for Security Evaluation
9. Defense-in-Depth Models— Rings of Protection

Enclave/Computing Environment

1. Peer-to-Peer Enclaves for Improving Network Defence
2. Practice List For Information Security Management
3. Error Handling, Auditing, Logging
4. Security Control Overlays for Industrial Control Systems V1 2013
5. A Report on the Privilege (Access) Management Workshop
6. Guide to Computer Security Log Management
7. Crowdsourcing Cyber Security: A Property Rights View of Exclusion and Theft on the Information Commons
8. Securing the Home Energy Management Platform Recommended

OWASP Mobile Security Project Testing Guide

Mobile Platform Security

1. Enhancing Java ME Security Support with Resource Usage Monitoring
2. Security
3. Understanding Symbian Platform Security

4. Ten Steps to Smartphone Security (Windows Phone)
5. Ten Steps to Smartphone Security for Apple iOS
6. IOS Application Security Testing Cheat Sheet
7. Android Security Terrorization
8. Formal Analysis of Security Models for Mobile Devices, Virtualization Platforms, and Domain Name Systems
   Mobile Protocols Security
   Mobile Application and Architecture Considerations
   Project 3 Step 2
   Mobile VPN Security
   Data at Rest
1. NIST Assessment Cases- System and Communications Protection- Protection of Data at Rest
   Data in Motion
   Project 3 Step 3
   Threat Agent Identification Example
   List of Threat Agents
   Project 3 Step 4
   Cyberattacks (Repeated for Convenience)
1. A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD
2. Collusion-Tolerable and Efficient Privacy-Preserving Time-Series Data Aggregation Protocol Recommended
3. Collusion-Resistant Audio Fingerprinting System in the Modulated Complex Lapped Transform Domain Recommended
4. Covert Encryption and Document Authentication Using Texture Coding Recommended
5. SQL Injection Prevention Cheat Sheet
6. Cache Poisoning
7. Robust Image Watermarking Theories and Techniques: A Review Recommended
8. OWASP Periodic Table of Vulnerabilities - Cookie Theft/Session Hijacking Recommended
9. Spoofing Attacks on Packets and Methods For Detection and Prevention of Spoofed Packets
10. Detection and Modeling of Cyber Attacks with Petri Nets
11. A Copyright Protection Scheme for Digital Images Based on Shuffled Singular Value Decomposition and Visual Cryptography Recommended
12. Dual Watermarking For High Protective Copyright System

13. DDoS Quick Guide Recommended
14. DRAFT Guide to Cyber Threat Information Sharing Recommended
15. Insecure Randomness Recommended
16. Digital Watermarking Recommended
17. Cyber Attacks Explained: Cryptographic Attacks
18. Testing for Padding Oracle Recommended
19. Stochastic Image Warping for Improved Watermark Desynchronization Recommended
20. Video Multiple Watermarking Technique Based on Image Interlacing Using DWT Recommended

Project 4

Project 4 Step 1

Security Development Life Cycle

Software Development Methodologies

1. Software Development Methodology
2. Agile Software Development
3. Waterfall Model
4. Joint Application Development (JAD)
5. Extreme Programming
6. Rapid Application Development (RAD)
7. Other Methods and Models
8. Check Your Knowledge (Test)

Critical Infrastructure Sectors

Process Control Systems: Cybersecurity and Defense

Threat Modeling

Project 4 Step 2

Software Quality Requirements Engineering (SQUARE)

1. Activity: Applying SQUARE

Project 4 Step 3

Database Models

Project 4 Step 4

Server Virtualization

Benefits and Features of Cloud Computing

Mobile Cloud Computing

Access Control (Repeated for Convenience)

1. Technological Safeguards
2. ID Management Issues and Requirements

3. NIST 800-53v4 (Pages F-7 through F-36)
4. An Introduction to Role-Based Access Control
5. Attribute-based access control
6. Database Security & Access Control Models: A Brief Overview
7. Access Control as a Service for the Cloud
8. Security Information in Production and Operations: A Study on Audit Trails in Database Systems
9. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid
10. RFID Privacy Risk Evaluation Based on Synthetic Method of Extended Attack Tree and Information Feature Entropy
11. Broken Access Control
12. Scientific World Journal Recommended
13. Dynamic Access Control Model for Security Client Services in Smart Grid Recommended
14. RFID Security Issues Recommended
15. Assessment of Access Control Systems Recommended
16. A Survey of Access Control Models Recommended
17. Cloud Multidomain Access Control Model Based on Role and Trust-Degree Recommended
18. Using Security Labels for Directory Access Control & Replication Control Recommended
19. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
20. Check Your Knowledge (Test)

Project 5

Project 5 Step 1

Security Concerns Common to All RDBMS

Project 5 Step 2

Error Handling and Information Leakage

1. The 13 System And Information Integrity Assessment Cases: SI 11 Error Handling
2. Handling Errors
3. Error Handling
4. OWASP Secure Coding Practice Guide

Insecure Handling (Repeated for Convenience)

1. WASC Threat Classification
2. Insecure Cryptographic Storage
3. Cyber Security Course: 19 Data in Transit. Learn Internet Security

4. Guide to Malware Incident Prevention and Handling for Desktops and Laptops
5. A Report on the Privilege (Access) Management Workshop
6. OWASP Backend Security
7. Industry Draft: NIST SP 800-118: Guide to Enterprise Password Management
8. Guide to Storage Encryption Technologies for End User Devices
9. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
10. Data Backup Options Recommended
11. NIST Assessment Cases- System and Communications Protection- Protection of Data at Rest Recommended

Cross-Site Scripting (XSS/CSRF) Flaws

1. You know about XSS. How about XSRF/CSRF?
2. Countermeasures

SQL Injections

Insecure Configuration Management

1. Using Wireless Technology Securely
2. Small Office/Home Office Router Security
3. Guide to Enterprise Patch Management Technologies
4. Guide to General Server Security
5. Insecure Configuration Management
6. Cyber Security Planning Guide
7. OWASP Backend Security
8. Recommended Practice for Patch Management of Control Systems
9. Guidelines on Firewalls & Firewall Policy
10. Guide to General Server Security
11. Guide for Security-Focused Configuration Management of Information Systems

Authentication (Repeated for Convenience)

1. NIST Special Publication 800-57 Part 1, Revision 3
2. How to Authenticate Users with API Keys
3. Key Management Cheat Sheet
4. User Authentication with OAuth 2.0
5. Centralized Authentication Using OpenLDAP
6. Message Authentication Codes
7. Has The Time Come to Kill the Password?
8. Towards Secure and Dependable Message Authentication in WSN Recommended
9. Message Authentication and Source Privacy in Wireless Networks Recommended
10. Biometrics Recommended
11. Security How-To: WPA2-Enterprise on Your Home Network Recommended

12. Production Best Practices: Security Recommended
13. Protecting Your System: User Access Security Recommended
14. Authentication Recommended
15. Top 10 2013-A2-Broken Authentication and Session Management Recommended
16. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
17. Activity: Message Authentication Recommended
18. Authentication Summary Recommended
19. Multifactor Authentication Overview Recommended
20. Authentication and Information Assurance Recommended
21. Check Your Knowledge (Test)

Access Control (Repeated for Convenience)

1. Technological Safeguards
2. ID Management Issues and Requirements
3. NIST 800-53v4 (Pages F-7 through F-36)
4. An Introduction to Role-Based Access Control
5. Attribute-based access control
6. Database Security & Access Control Models: A Brief Overview
7. Access Control as a Service for the Cloud
8. Security Information in Production and Operations: A Study on Audit Trails in Database Systems
9. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid
10. RFID Privacy Risk Evaluation Based on Synthetic Method of Extended Attack Tree and Information Feature Entropy
11. Broken Access Control
12. Scientific World Journal Recommended
13. Dynamic Access Control Model for Security Client Services in Smart Grid Recommended
14. RFID Security Issues Recommended
15. Assessment of Access Control Systems Recommended
16. A Survey of Access Control Models Recommended
17. Cloud Multidomain Access Control Model Based on Role and Trust-Degree Recommended
18. Using Security Labels for Directory Access Control & Replication Control Recommended
19. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
20. Check Your Knowledge (Test)

Project 5 Step 3

Database Models
Common Criteria (CC) For Information Technology Security Evaluation

1. National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Briefing to IAPB
2. A Common Criteria Primer
3. COTS Security Protection Profile-Operating Systems
4. Evaluation Assurance Levels for Human Resource Security of an Information System
5. Operating System Protection Profile

Evaluated Assurance Levels (EALs)

1. Authentication and Information Assurance
2. Operating System Protection Profile

Continuity of Service

1. Business Continuity & Disaster Recovery Planning Domain
2. Writing a Business Continuity Plan
3. The Definitive Backup Guide
4. Backup and Recovery
5. Trusted Recovery From Information Attacks
6. Trusted Recovery
7. Backups, Redundancy, and the Cloud

Threats

1. Mobile Threats-Device Based Threat Vectors
2. Network-Based Threat Vector
3. Check Your Knowledge (Test)

Project 5 Step 4

Defensive Principles
Enclave/Computing Environment (Repeated for Convenience)

1. Peer-to-Peer Enclaves for Improving Network Defence
2. Practice List For Information Security Management
3. Error Handling, Auditing, Logging
4. Security Control Overlays for Industrial Control Systems V1 2013
5. A Report on the Privilege (Access) Management Workshop
6. Guide to Computer Security Log Management
7. Crowdsourcing Cyber Security: A Property Rights View of Exclusion and Theft on the Information Commons
8. Securing the Home Energy Management Platform Recommended

Cyber Operations in DoD policy and Plans

1. Cyber Operations in DOD Policy and Plans
2. Cyber Strategy – Department of Defense
3. Check Your Knowledge (Test)

Project 5 Step 7

Operating System Security (Repeated for Convenience)

1. System and Kernel Security
2. How To Use the Linux Auditing System on CentOS 7
3. Ring (Computer Security)
4. Operating Systems Security: Protection Measures Analysis
5. A Security Adaptation Reference Monitor for Wireless Sensor Network
6. Security: An Advanced Introduction
7. Error Handling, Auditing, and Logging
8. Using Proven Reference Monitor Patterns for Security Evaluation
9. Defense-in-Depth Models— Rings of Protection

Trusted Computing

1. Trusted Platform Module (TPM)
2. Introduction to Trusted Computing: TPM 101
3. Trusted Computing: Promise and Risk
4. A Survey on Authentication Techniques and User Recognition
5. Protecting Systems with the TPM
6. Protect Your Information from Physical Threats
7. Multiagent Systems Protection
8. Trusted Computing Strengthens Cloud Authentication
9. User Authentication
10. Memory Protection

Trusted Computing Base

1. Trusted Computing Strengthens Cloud Authentication
2. A Mobile and Portable Trusted Computing Platform
3. Inter-Process Communication
4. Memory Protection

Project 5 Step 8

Access Control (Repeated for Convenience)

1. Technological Safeguards
2. ID Management Issues and Requirements
3. NIST 800-53v4 (Pages F-7 through F-36)
4. An Introduction to Role-Based Access Control
5. Attribute-based access control

6. Database Security & Access Control Models: A Brief Overview
7. Access Control as a Service for the Cloud
8. Security Information in Production and Operations: A Study on Audit Trails in Database Systems
9. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid
10. RFID Privacy Risk Evaluation Based on Synthetic Method of Extended Attack Tree and Information Feature Entropy
11. Broken Access Control
12. Scientific World Journal Recommended
13. Dynamic Access Control Model for Security Client Services in Smart Grid Recommended
14. RFID Security Issues Recommended
15. Assessment of Access Control Systems Recommended
16. A Survey of Access Control Models Recommended
17. Cloud Multidomain Access Control Model Based on Role and Trust-Degree Recommended
18. Using Security Labels for Directory Access Control & Replication Control Recommended
19. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
20. Check Your Knowledge (Test)

Authentication (Repeated for Convenience)

1. NIST Special Publication 800-57 Part 1, Revision 3
2. How to Authenticate Users with API Keys
3. Key Management Cheat Sheet
4. User Authentication with OAuth 2.0
5. Centralized Authentication Using OpenLDAP
6. Message Authentication Codes
7. Has The Time Come to Kill the Password?
8. Towards Secure and Dependable Message Authentication in WSN Recommended
9. Message Authentication and Source Privacy in Wireless Networks Recommended
10. Biometrics Recommended
11. Security How-To: WPA2-Enterprise on Your Home Network Recommended
12. Production Best Practices: Security Recommended
13. Protecting Your System: User Access Security Recommended
14. Authentication Recommended
15. Top 10 2013-A2-Broken Authentication and Session Management Recommended

16. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
17. Activity: Message Authentication Recommended
18. Authentication Summary Recommended
19. Multifactor Authentication Overview Recommended
20. Authentication and Information Assurance Recommended
21. Check Your Knowledge (Test)

Multiple Independent Levels Of Security (MILS)

1. Formal Specification and Verification of Data Separation in a Separation Kernel for an Embdedded System
2. A Secure System Architecture for Measuring Instruments in Legal Metrology; See Background Sections
3. Implications of Multi-Core Architectures on the Development of Multiple Independent Levels of Security (MILS) Compliant Systems
4. A New Operating System for Security Tagged Architecture Hardware in Support of Multiple Independent Levels of Security (MILS) Compliant System

Cybersecurity Models

1. Cybersecurity Models
2. Clark-Wilson Model
3. The Biba Integrity Model
4. Biba's Strict Integrity Policy Model
5. Noninterference Model
6. Graham-Denning Model
7. Bell-LaPadula Model
8. Bell LaPadula Model Part 1
9. Chinese Wall Model
10. Deducibility Security
11. Clinical Information Systems Security Model
12. Check Your Knowledge

Insecure Handling (Repeated for Convenience)

1. WASC Threat Classification
2. Insecure Cryptographic Storage
3. Cyber Security Course: 19 Data in Transit. Learn Internet Security
4. Guide to Malware Incident Prevention and Handling for Desktops and Laptops
5. A Report on the Privilege (Access) Management Workshop
6. OWASP Backend Security
7. Industry Draft: NIST SP 800-118: Guide to Enterprise Password Management
8. Guide to Storage Encryption Technologies for End User Devices

9. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
10. Data Backup Options Recommended
11. NIST Assessment Cases- System and Communications Protection- Protection of Data at Rest Recommended

Project 5 Step 9

Access Control (Repeated for Convenience)

1. Technological Safeguards
2. ID Management Issues and Requirements
3. NIST 800-53v4 (Pages F-7 through F-36)
4. An Introduction to Role-Based Access Control
5. Attribute-based access control
6. Database Security & Access Control Models: A Brief Overview
7. Access Control as a Service for the Cloud
8. Security Information in Production and Operations: A Study on Audit Trails in Database Systems
9. State of the Art Authentication, Access Control, and Secure Integration in Smart Grid
10. RFID Privacy Risk Evaluation Based on Synthetic Method of Extended Attack Tree and Information Feature Entropy
11. Broken Access Control
12. Scientific World Journal Recommended
13. Dynamic Access Control Model for Security Client Services in Smart Grid Recommended
14. RFID Security Issues Recommended
15. Assessment of Access Control Systems Recommended
16. A Survey of Access Control Models Recommended
17. Cloud Multidomain Access Control Model Based on Role and Trust-Degree Recommended
18. Using Security Labels for Directory Access Control & Replication Control Recommended
19. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
20. Check Your Knowledge (Test)

Authentication (Repeated for Convenience)

1. NIST Special Publication 800-57 Part 1, Revision 3
2. How to Authenticate Users with API Keys
3. Key Management Cheat Sheet
4. User Authentication with OAuth 2.0

5. Centralized Authentication Using OpenLDAP
6. Message Authentication Codes
7. Has The Time Come to Kill the Password?
8. Towards Secure and Dependable Message Authentication in WSN Recommended
9. Message Authentication and Source Privacy in Wireless Networks Recommended
10. Biometrics Recommended
11. Security How-To: WPA2-Enterprise on Your Home Network Recommended
12. Production Best Practices: Security Recommended
13. Protecting Your System: User Access Security Recommended
14. Authentication Recommended
15. Top 10 2013-A2-Broken Authentication and Session Management Recommended
16. OWASP Top 10 for .NET Developers Part 3: Broken authentication and Session Management Recommended
17. Activity: Message Authentication Recommended
18. Authentication Summary Recommended
19. Multifactor Authentication Overview Recommended
20. Authentication and Information Assurance Recommended
21. Check Your Knowledge (Test)

Direct Object Access

1. OWASP Top 10 for .NET Developers Part 6: Security Misconfiguration
2. Building a LAMP Server
3. OWASP Top 10 for .NET Developers Part 4: Insecure Direct Object Reference
4. OWASP Top 10 for .NET Developers Part 10: Unvalidated Redirects and Forwards
5. The Ruby UCSC API: Accessing the UCSC Genome Database Using Ruby
6. Defending vulnerable security protocols by means of attack interference in non-collaborative scenarios
7. Practical Attacks on Mobile Cellular Networks and Possible Countermeasures
8. Grid-Control Post Implementation Configuration Guide

Project 5 Step 10

Guidelines for a Test and Remediation Results (TPRR) Report