CS-6035 Intro to Information Security
Course Textbook

Welcome to CS-6035,

The Graduate Introduction to Information Security (or IIS) is a fascinating subject and a wonderful course to start your careers as cyber security professionals. This course is hard, and technology changes often. One of our goals with this course is to give you the tools and intuition to reason your way through the cybersecurity incidents of the past and the present.

When we first came to this course many years ago it came with a textbook requirement. Like many courses before it, the questions arose of whether the latest edition was required; indistinguishable from the one before. Not everyone has the money for textbooks, and we're not interested in making it harder for those on a path of learning. The field of cybersecurity has benefitted greatly from open-source, and as you study this field, you will learn that is a matter of liberty, not price. We should live this as educators as well.

Therefore, in the interest of increasing the availability of the course for students, we've moved the textbook to a collection of online and open-source materials. This approach comes with a number of benefits:

- The resources get the exposure that the volunteers who created them deserve
- As they're used, they will be improved by the students using them and making contributions
- They are available, free of charge, to anyone

As you struggle through the course material, treat this book as you would any other resource. It is a starting point, not an ending point. If you find errors in the materials, submit improvements. If you find faults, give solutions. We'll be here to improve this collection of resources throughout the semesters to keep the course up to date and the material ever more constructive.

We wish you the best of luck.

Sincerely,
The IIS Instructional Team

Table of Contents :

This page unintentionally, but then intentionally, left blank

Chapters:

Chapter 1: Overview & Computing Concepts

- The OSTEP Textbook Intro Chapter on Operating System Security

Chapter 2: Cryptographic Tools

- The OSTEP Textbook Chapter on Protecting Information With Cryptography
- Key Management - OWASP Cheat Sheet Series

Chapter 3: User Authentication

- The OSTEP Textbook Chapter on Authentication
- Authentication - OWASP Cheat Series
- Password Storage - OWASP

Chapter 4: Access Controls

- The OSTEP Textbook Chapter on Access Control
- https://owasp.org/www-community/Access_Control
- Broken Access Control for Software Security | OWASP Foundation

Chapter 5: Database and Data Center Security

- Database Security - OWASP Cheat Sheet Series
- Database Encryption – An Overview of Contemporary Challenges and Design Considerations
- A Classification of SQL Injection Attacks and Countermeasures
- SQL Injection Attacks and Defense | Chapter 1 is enough for our purposes
- Access Control: Principles and Practice
- Access Control: Policies, Models, and Mechanisms

Chapter 6: Malicious Software

- Spyware Software Attack | OWASP Foundation
- Types of Malware
- 22 Types of Malware and How They Spread
- Malware Propagation and Prevention

- Malware Prevention
- 10 Tips for Malware Prevention
- Computer Worm Classification
- The Morris Worm (1988)
- The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability
- Keylogger Detection and Prevention
- A Brief Survey on Rootkit Techniques in Malicious Codes
- Countermeasures to Ransomware Threats
- Guide to Malware Incident Prevention and Handling
- Malware in Motion
- You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger
- A Taxonomy of Computer Worms
- Worm Propagation Model
- Clickjacking
- The Stuxnet Story: What really happened at Natanz
- What is a Logic Bomb?
- OWASP Automated Threats to Web Applications
- An Introduction to Hardware-Assisted Virtual Machine (HVM) Rootkits
- Evolution and Detection of Polymorphic and Metamorphic Malwares: A Survey

Videos

- Botnets - Computerphile
- The Stuxnet Story: What really happened at Natanz

Chapter 7: Denial of Service Attacks

- Network Denial of Service, Technique T1498 - Enterprise | MITRE ATT&CK
- Distributed Denial of Service Attack and Defence
- DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art
- Analysis of a Denial of Service Attack on TCP
- HTTP Attack Detection Using N-gram Analysis
- DDoS attack algorithm using ICMP flood
- Improve SDN Responsiveness to UDP Flood Attacks
- SAFETY: Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN
- SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design

Videos

- DDoS Attacks as Fast As Possible
- The Attack That Could Disrupt The Whole Internet - Computerphile
- DDoS Attacks - An Explanation of Amplified Reflective UDP-based Attacks

Chapter 8: Intrusion Detection

- Intrusion Detection Control | OWASP Foundation
- Intrusion Detection Systems

- Personal Firewalls and Intrusion Detection Systems

Chapter 9: Firewalls and Intrusion Detection

- Web Application Firewall | OWASP Foundation
- Firewalls and Beyond
- This simple blog post from AWS on DOS protection with WAFs
- Microsoft Word - intro_firewalls.doc (routeralley.com)
- Intrusion Detection Basics - SmallNetBuilder
- Importance_of_Intrusion_Detection_System (ijser.org)
- (PDF) Firewalls, Intrusion Detection and Anti-virus Scanners | Julie Greensmith - Academia.edu
- Survey of intrusion detection systems: techniques, datasets and challenges | Cybersecurity | Full Text (springeropen.com)

Chapter 10: Buffer Overflows

- Buffer Overflow | OWASP Foundation
- Buffer Overflow Software Attack | OWASP Foundation
- Buffer Overflow via Environment Variables | OWASP Foundation
- Intel Software Developer Manual
    - Section 3.4 - 3.4.1.1
    - Section 3.5, 3.5.1
    - Section 4.1 - 4.2.1.2
    - Section 4.3 - 4.3.1
    - Section 5.1.13
    - Section 6.1 - 6.2.5
    - Section 6.4 - 6.4.3.3

Chapter 11: Software Security

- SQL Injection | OWASP Foundation
- A small resource on signature based SQL injection
- Improper Data Validation | OWASP Foundation
- Smashing the Stack for Fun and Profit
- Entropy - OWASP

Chapter 12: Operating system security

- https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html
- OS Security Basics
- Windows OS Security
- Linux Security
- Virtualization Security - Kaspersky Labs
- What is the difference between Type 1 and Type 2 Hypervisor

Chapter 13: Cloud and IoT security

- OSTEP Ch. 57
- A Comprehensive Survey on Security in Cloud Computing
- Towards Security on Internet of Things: Applications and Challenges in Technology

Chapter 14: IT Security Management and risk assessment

- Threat Modeling | OWASP Foundation
- Security Intelligence on Simplifying Risk Management
- Risk Management Guide for Information Technology Systems
- OWASP Risk Assessment Framework
- Cybersecurity Risk Management | Frameworks, Analysis & Assessment | Imperva
- guide_to_cybersecurity_as_risk_management_the_role_of_elected_officials_0.pdf (cgi.com)

Chapter 15: IT security controls

- What are security controls
- ISO/IEC 27002 security controls
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
  - Chapters 1-3
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://engage.mitre.org/matrix/
- https://attack.mitre.org/mitigations/enterprise/

Chapter 16: Legal and Ethical aspects

- Legal
  - Legal Aspects of Cybersecurity
  - USA Federal Laws in Cybersecurity 2022
  - US Copyright Office Summary of the Digital Millennium Copyright Act

- Intellectual Property
  - 5 insights on cyberattacks and intellectual property
  - IPCybersecurity.com

- Ethics
  - Moral Responsibility for Computing Artifacts: “The Rules”
  - Ethics in cybersecurity research and practice - Paper
  - Ethics and Cybersecurity are not Exclusive - Paper

Chapter 17: Symmetric Encryption and message confidentiality

- http://paper.ijcsns.org/07_book/201901/20190107.pdf – note this paper is published by a publisher on a predatory journal list, but it's still useful information, so we left it – JL
- https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-symmetric-cryptography

Chapter 18: public-key cryptography and message authentication

- We recommend OMSCS Student George K.'s notes on cryptography https://teapowered.dev/assets/crypto-notes.pdf
- https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-public-key-cryptography

Chapter 19: Internet Security Protocols and Standards

- Internet Security Cryptographic Principles, Algorithms and Protocols
- IPV4/IPV6 SECURITY AND THREAT COMPARISONS
- DKIM, DMARC, and other email security methods
- Common ways organizations implement and break Internet Security Protocols:
  - Encrypt Sensitive Information
  - SSL/TLS Inspection and common mitigation strategies

Chapter 20: Internet Authentication Applications, Internet Security & Cryptographic Principles

- The Three A's of of Access Control
- How file permissions work
- Kerberos: An Authentication Service for Computer Networks
- RBAC: Role-Based Access Control Explained!
- Public Key Infrastructure
- Public Key Infrastructure PKI Concepts
- Stanford cs140's lecture on Access Control
- Understand Discretionary Access Control (DAC)

Chapter 21: Wireless Network Security

- How does HTTPS Actually Work by Robert Heaton
- Wireless Network Security: Challenges, Threats and Solutions. A Critical Review – note this paper is published by a publisher on a predatory journal list, but it's still useful information, so we left it – JL
- Mobile Device Security
- Wireless LAN Security Threats and Vulnerabilities (page 189)
  - Section beginning on page 189

Chapter 22: Trusted Computing & Multilevel Security

- If A1 is the Answer, What was the Question? An Edgy Naïf's Retrospective on Promulgating the Trusted Computer Systems Evaluation Criteria
- Reflections on Trusting Trust
- BUILDING A SECURE COMPUTER SYSTEM
  - Chapters 1, 3, 5, and 6
- The ten-page introduction to *Trusted Computing*

- The Trusted Computing Base (material for the CISSP, but well explained)
- The Future of Multi-Level Secure (MLS) Information Systems
- Security Engineering: A Guide to Building Dependable Distributed Systems

Additional Project Resources:

Research papers and Assigned Readings

You can find our assigned research papers for the course projects in this folder

As a note for students, like the title says, these additional project resources are not required for the course, they are optional. You are not required to know everything in each of these resources.

We're happy to take any recommendations on fantastic open source resources that helped you learn for any of the projects.

Project 1

Academic Papers

- Shacham, H. (2007, October). "The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls. Hovav.net. https://hovav.net/ucsd/papers/s07.html
- Jiang et al. (2010, April 22). Jump-Oriented Programming: A New Class of Code-Reuse Attack. ASIACCS. www.academia.edu/909994/Jump-oriented_programming_A_new_class_of_code-reuse_attack

Web Pages and Articles

- TutotialsPoint. (2016, June). Assembly - Sytem Calls. www.tutorialspoint.com/assembly_programming/assembly_system_calls.htm
- Lea, D. (2001, March 11). Malloc implementation for multiple threads without lock contention. Sourceware. http://sourceware.org/git/?p=glibc.git;a=blob_plain;f=malloc/malloc.c
- c0ntex. (unknown). Bypassing non-executable-stack during exploitation using return-to-libc. MIT. http://css.csail.mit.edu/6.858/2017/readings/return-to-libc.pdf
- Mazzocchio, D. (2006, April 26). Writing Shellcode for Linux and BSD - Writing the Shellcode. Kernel Panic. www.kernel-panic.it/security/shellcode/shellcode4.html
- Hanna, S. (2007, June). Shellcoding for Linux and Windows Tutorial. Vividmachines. https://vividmachines.com/shellcode/shellcode.html
- Tenouk. (unknown). BUFFER OVERFLOW 6 - The Function Stack. Tenouk. https://www.tenouk.com/Bufferoverflowc/Bufferoverflow2a.html
- Bendersky, E. (2011, February 4). Where the top of the stack is on x86. TheGreenPlace. https://eli.thegreenplace.net/2011/02/04/where-the-top-of-the-stack-is-on-x86/
- Khonig, A. (2012, April 3). All About EBP. Running the Gauntlet. https://practicalmalwareanalysis.com/2012/04/03/all-about-ebp/
- Drake, D. and Berg, J. (unknown). Unaligned Memory Accesses. Linux Kernel Archives. https://www.kernel.org/doc/Documentation/unaligned-memory-access.txt
- Kahan, Z. (2013, May 6). ROP (Return Oriented Programming) - The Basics. Zolmeister. https://zolmeister.com/2013/05/rop-return-oriented-programming-basics.html
- Brouwer, A. (2003, April 1). 11. Exploiting the heap. Hackers Hut. https://www.win.tue.nl/~aeb/linux/hh/hh-11.html
- Software Engineering. (2013, April 18). Understanding stack frame of function call in C/C++? StackExchange. https://softwareengineering.stackexchange.com/questions/195385/understanding-stack-frame-of-%20function-call-in-c-c

Videos

- Slater, D. (2015, November 11). How to exploit a buffer overflow vulnerability - Practical. YouTube. https://www.youtube.com/watch?v=hJ8IwyhqzD4
- Lyne, J. (2015, March 25). How They Hack: Buffer Overflow & GDB Analysis. YouTube. https://www.youtube.com/watch?v=V9lMxx3iFWU
- Computerphile. (2016, March 2). Running a Buffer Overflow Attack. YouTube. https://www.youtube.com/watch?v=1S0aBV-Waeo

Project 2

Academic Papers

- Rossow, C. et al. (2012, May 20). Prudent Practices for Designing Malware Experiments: Status Quo and Outlook. IEEE Xplore. https://ieeexplore.ieee.org/document/6234405?arnumber=6234405
- Graziano, M. et al. (2015, August 12). Needles in a Haystack: Mining Information from Public Dynamic Analysis Sandboxes for Malware Intelligence. Usenix. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-graziano.pdf

Web Pages and Articles

- Cuckoo Foundation. (2010). Cuckoo Introduction. Read the Docs. https://cuckoo.readthedocs.io/en/latest/introduction/
- Lee, W. (2019). Malware and Attack Technologies Knowledge Area - Issue 1.0. Cybok. https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf
- Kuar, N. and Bindal, A. (2016, Feburary 4). A Complete Dynamic Malware Analysis. International Journal of Computer Applications Volume 135. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.5517&rep=rep1&type=pdf
- Santos, I. et al. (unknown). N-GRAMS-BASED FILE SIGNATURES FOR MALWARE DETECTION. CiteSeerX. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.517.6882&rep=rep1&type=pdf

Videos

- Fox, N. (2020, August 5). #5 Malware Analysis Using a Cuckoo Sandbox. YouTube. https://www.youtube.com/watch?v=7Nm48OQWmA8&t=95s
- DecisionForest. (2020, March 25). What are Unigrams, Bigrams & N-Grams - N-Gram Analysis for Machine Learning Projects. YouTube. https://www.youtube.com/watch?v=MZIm_5NN3MY

Project 3

Academic Papers

- Shamir, A., and Tromer, E. (2003). On the cost of factoring RSA-1024. RSA CryptoBytes, 6(2), 10-19. http://www.cs.tau.ac.il/~tromer/papers/cbtwirl.pdf
- da Silva, J. C. L. (2010, November). Factoring semiprimes and possible implications for RSA. In 2010 IEEE 26-th Convention of Electrical and Electronics Engineers in Israel (pp. 000182-000183). IEEE. https://ieeexplore.ieee.org/abstract/document/5661953

Web Pages and Articles

- Sweigart, A. (2009). Hacking Secret Ciphers with Python - Chapter 23 - Finding Prime Numbers. Invent With Python. https://inventwithpython.com/hacking/chapter23.html

- Sweigart, A. (2009). Hacking Secret Ciphers with Python - Chapter 24 - Public Key Cryptography and the RSA Cipher. Invent With Python. https://inventwithpython.com/hacking/chapter24.html
- Stack Overflow. (2011, June 6.) Program to factorize a number into two smaller prime numbers. https://stackoverflow.com/questions/6254078/program-to-factorize-a-number-into-two-smaller-prime-numbers
- Sullivan, C. and Makmur, R. (1996, June 12). RSA Algorithm Javascript Page. University of Pittsburgh. https://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/
- Khan Academy. (unknown). Modular inverses. Modular arithmetic. https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-inverses
- Vegaseat. (2007, March 4). Check if a number is a prime number (Python). Daniweb. https://www.daniweb.com/programming/software-development/code/216880/check-if-a-number-is-a-prime-number-python
- Stack Exchange. (2017, October 24). Deciphering the RSA encrypted message from three different public keys. https://crypto.stackexchange.com/questions/52504/deciphering-the-rsa-encrypted-message-from-three-different-public-keys
- Stack Exchange. (2011, March 1). Should RSA public exponent be only in {3, 5, 17, 257 or 65537} due to security considerations? https://security.stackexchange.com/questions/2335/should-rsa-public-exponent-be-only-in-3-5-17-257-or-65537-due-to-security-c
- Wikipedia. (2014, December 19). Coppersmith's Attack. https://en.wikipedia.org/wiki/Coppersmith%27s_attack#H%C3%A5stad's_broadcast_attack
- Wood, T. (unknown). What is the F-score? DeepAI. https://deepai.org/machine-learning-glossary-and-terms/f-score
- Nakamoto, S. (unknown). Bitcoin: A Peer-to-Peer Electronic Cash System. BitCoin.org. https://bitcoin.org/bitcoin.pdf

Videos

- 3Blue1Brown. (2017, July 7). But how does bitcoin actually work? YouTube. https://www.youtube.com/watch?v=bBC-nXj3Ng4
- Khan Academy. (unknown). RSA encryption: Step 1. https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/intro-to-rsa-encryption

Project 4

Academic Papers

- Jain, S. (2016). Explorative Study of SQL Injection Attacks and Mechanisms to Secure Web Application Database- A Review. Academia. https://www.academia.edu/65589560/Explorative_Study_of_SQL_Injection_Attacks_and_Mechanisms_to_Secure_Web_Application_Database_A_Review
- Tajpour, A. (2010). Evaluation of SQL Injection Detection and Prevention Techniques. Academia. https://www.academia.edu/62200112/Evaluation_of_SQL_Injection_Detection_and_Prevention_Techniques
- Sarmah, U. et al. (2018, June 4). A Survey of Detection Methods for XSS Attacks. University of Colorado - Colorado Springs.

http://cs.uccs.edu/~jkalita/papers/2018/UpasanaSarmahIJCNA2018.pdf

- Sentamilselvan K. (2013, March). Survey on Cross Site Request Forgery (An Overview of CSRF). ResearchGate. https://www.researchgate.net/publication/281583832_Survey_on_Cross_Site_Request_Forgery_An_Overview_of_CSRF

Web Pages and Articles

- W3Schools. (1999). SQL Injection. https://www.w3schools.com/sql/sql_injection.asp
- W3Schools. (1999). Javascript Tutorial. https://www.w3schools.com/js/
- OWASP Cheat Sheet Series. (unknown). SQL Injection Prevention Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- OWASP Cheat Sheet Series. (unknown). HTML5 Security Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#Cross_Origin_Resource_Sharing
- KirstenS. (unknown). Cross Site Request Forgery (CSRF). OWASP. https://owasp.org/www-community/attacks/csrf
- Wikipedia. (2003, June 6). Cross-site scripting. https://en.wikipedia.org/wiki/Cross-site_scripting
- Bughunters. (unknown). Welcome to Bug Hunter University. Google. https://bughunters.google.com/learn
- Kallin, J. and Valbuena, I. (2013). Excess XSS - Part One: Overview. Excess XSS. https://excess-xss.com/
- PHP Manual. (unknown). PHP - Double Quoted. https://www.php.net/manual/en/language.types.string.php#language.types.string.syntax.double
- PHP. (unknown). Prepared statements and stored procedures. https://www.php.net/manual/en/pdo.prepared-statements.php
- Bobby Tables. (unknown). Bobby Tables: A guide to preventing SQL injection - PHP. https://bobby-tables.com/php

Videos

Appendix:

Additional Resources:

The majority of the resources from this book are sourced from :

- OWASP Community Pages
- OWASP Cheat Sheet Series
- Operating Systems: Three Easy Pieces
- DEFEND Knowledge Graph

Special Thanks:

This textbook wouldn't have been possible without the courage and effort of so many individuals, we mention some of them here.

- Professor Wenke Lee
- Head TA Chris Taylor
- The IIS TA Team
- Pablo Ximinez
- George Kudrayvtsev
- The Stichting Cuckoo Foundation for their work on Cuckoo and malware analysis