CSC 564 Computer Security

Fall 2014

This syllabus is a guideline for the course and not a contract. As such, its terms may be altered when doing so is, in the opinion of the instructor, in the best interests of the class.

General Information

Professor: Sviatoslav (Svet) Braynov
Office: UHB 3117
Email: sbray2@uis.edu (for a faster response please put "CSC564" in the subject)
Lectures: W, 8:00 pm - 9:40 pm, UHB 2032
Office Hours: MW, 5:00 pm - 6:00 pm. You don't need an appointment to see me if I am in my office. Please feel free to come any time!

Course Overview

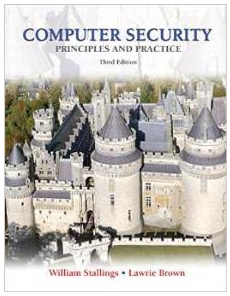
The intensive growth of the Internet has spawned an increased awareness in security issues. This course provides students with a background, foundation, and insight into the subject of Computer Security at a graduate level.

Course objectives

This course calls on students to demonstrate:

- Knowledge of security technologies, applications, and concepts,
- The ability to reason through analysis, evaluation and design of secure systems,
- The ability to effectively apply this knowledge to the construction of secure software systems.

Textbook



Computer Security: Principles and Practice, by William Stallings and Lawrie Brown, Pearson Education/Prentice Hall, 2nd edition, 2012, ISBN-10: 0132775069.

Other useful textbooks (optional):

- Introduction to Computer Security by Miachel Goodrich and Roberto Tamassia, Addison Wesley, 2011. ISBN: 0-321-51294-4

Topics covered in class

1. **An overview of computer security.**

   Computer Security Concepts. Confidentiality, Integrity, and Availability. Threats, attacks and assets. Computer Security Challenges. Characteristic of Intrusions. Method, Opportunity, and Motive. Computer Criminals. Countermeasures. Security Functional Requirements. Fundamental Security Design Principles, Attack Surfaces and Attack Trees.X.800 Security Architecture. Security Trends. Computer Security Strategy. Policy and Mechanism. Assurance.

2. **Introduction to cryptography.**

   Cryptographic Concepts. Cryptosystem. Attacks on Cryptosystems. Kerckhoff's Principles. Unconditional and computational Security. Symmetric Cryptosystems. Symmetric Key Distribution. Public-Key Cryptography. Public Key Distribution. Digital Signatures. Cryptographic Hash Functions. Trapdoor function. Message Authentication Codes. Digital Certificates.

3. **Brief History of Cryptography**

   Monoalphabetic cipher. Cryptanalysis of Caesar Cipher. Language Redundancy and Cryptanalysis. Frequency Analysis. Additive Ciphers. Multiplicative Ciphers. Affine Ciphers. Homophonic substitution cipher. Substitution Boxes. Polyalphabetical ciphers. Autokey cipher. Playfair Cipher. Vigenère Cipher. Vernam Cipher. One-Time Pads. Project Venona. Transposition Ciphers. Hill Cipher. Rotor Machines. Product Ciphers. Block vs. stream ciphers. Padding. PKCS5. Shannon's Characteristics of good ciphers. Diffusion and confusion.

4. **Data Encryption Standard**

   History of DES. Feistel Cipher Structure. DES Design Controversy. Initial Permutation. The f Function. Expansion permutation. S-Boxes. Diffusion. Characteristics of DES. Triple DES. Meet in the Middle Attack.

5. **Advanced Encryption Standard**

   History of AES. Byte Substitution. Shift Rows. MixColumns. RoundKeyAddition. The key schedule. Modes of Operation. Electronic Codebook Mode. Cipher Block Chaining Mode. Cipher Feedback Mode. Cipher Feedback Mode. Counter Mode.

6. **A Crash Course into Basic Number Theory**

   Divisibility. Fundamental Theorem of Arithmetic. Greatest Common Divisor. The Euclidian Algorithm. Congruences. The inverse. Modular exponentiation. Fermat's Little Theorem. Euler's Theorem.

7. RSA

Description and mathematical proofs. How to choose good p and q. Attacks on RSA. Timing attacks. Defenses against timing attacks.

8. **Diffie-Hellman agreement**

Description. Man-in-the-middle attack.

9. **Introduction to Public Key Infrastructure (PKI)**

Keys have limited lifetimes. The lifecycle of a key. Key-Pair Generation. Private Key Storage. Certification authority (CA). Simple Public-Key Certificate. Certificate's properties. Types of certificates. Certification Path. Certificate Distribution via Directory Services. X.509 Certificate Format. X.500 Names. Abstract Syntax Notation One. VeriSign Certificates. NetSure protection. Certificate revocation. Certificate Revocation Lists. CRL distribution. Short-Lived Certificates.

10. **Electronic contracts and digital signatures**

E-SIGN. Contract law and signatures. Contracts that do not require signatures. Birthday paradox.

11. Minimal Disclosure Certificates and Zero-knowledge proofs

12. Message Authentication

Message encryption. Message Authentication Codes. Hash functions. One-way functions. Hash Function Requirements. Weak and Strong collision resistance. Message Digest Functions. Hash function with symmetric encryption. Hash function with asymmetric encryption. Hash function with asymmetric + symmetric encryption. Hash function with a secret value. Hash function with a secret value and symmetric encryption. Internal error control. External error control. MAC Properties. Requirements for MACs. MAC without confidentiality. MAC with confidentiality. Data Authentication Algorithm.

13. Steganography

History of Steganography. Basic terminology. Basic Requirements. Text Steganography. Substitution Systems. Least significant bit substitution. Random interval method. Image downgrading. Parity bits and cover regions. Palette-based techniques. Pure steganography. Secret key steganography. Public key steganography. Security of steganography system. Adaptive vs. nonadaptive algorithms. Supraliminal channels. Robustness. Spread spectrum techniques. Generation of English sentences. DNA-based Steganography.

14. Digital Watermarking

History of Watermarking. Basics of Digital Watermarking. Visible and Invisible Watermarks. Fragile watermarks. Robust watermarks. Fingerprints. Applications: Broadcast Monitoring, Owner identification, Transaction tracking, Content authentication, Copy Control, Device control.

15. **User authentication**

Means of User Authentication. Password Authentication. Password Vulnerabilities. Use of Hashed Passwords. UNIX Implementation. Improved Implementations. Windows implementation. Password Cracking. Password File Access Control. Password selection criteria. How to remember strong passwords. Proactive Password Checking – Bloom filter and Markov models. Token Authentication. Smartcards. One-time passwords.

16. **Challenge-response systems**

Based on symmetric cipher and a nonce. Based on a time stamp. Bidirectional authentication. Based on MAC and a timestamp. Based on public cipher. Using digital signature.

17. **Graphical passwords**

Types of graphical passwords. Dual-code theory. Image recognition. Face scheme. Story scheme. Tapping or drawing. Signature drawn. Graphical password resistant to shoulder surfing.

18. **Biometrics**

Physiological and behavioral biometrics. Fingerprint Patterns. Palm print. Vein pattern. Hand geometry. Finger geometry. Retina. Iris. Facial. Voice. Signature. Typing Dynamics. Biometrics for identification. Biometrics for verification. Performance Metrics. Biometric Accuracy. Approximate Message Authentication Codes (AMACs). Types of Algorithms for Facial Interpretation. Eigenface. Local feature analysis. Neural networks.

19. **Physical security**

The basics of physical security. Destructive vs. Nondestructive Entry. Direct Attacks on Computational Devices . Environmental Attacks . Eavesdropping . Wiretapping. Signal Eminations. Hardware Keyloggers. TEMPEST. Emanation Blockage. Faraday Cages.

20. **Locks, Keys and Lock Picking**

Compromising Locks. Lock Picking. Lock types. TSA lock. Warded Locks. Skeleton Key. Pick vs. Bypass. 1860: Yale Pin Tumbler Lock. How Does a Pin Tumbler Lock Work? Wafer tumbler locks. Combination Locks. Electronic combination locks. Safes. Basic terminology of lock picking. Lockpicking Tools. Feeler Picking. Scrubbing / Raking. Bumping. Bump Keys. Pick Gun. The Math of Lock Picking. Rights Amplification in Master Keyed Systems. Rights Amplification Statistics. Side Channel Attacks.

21. **Fingerprint biometrics**

Ridge patterns. Arches. Loops. Whorls. Orientation. Spatial frequency. Curvature. Position. Core point. Delta point. Ridge count. Ridge ending. Ridge bifurcation. Ridge divergence. Dot and islands. Enclosures and lakes. Short ridges. Attacking the Physical Finger.

22. **SSL**

SSL/TLS Features. SSL Architecture. SSL Record Protocol. SSL Alert Protocol. ChangeCipherSpec Protocol. Handshake protocol and Handshake Messages. Master secret. Key block.

23. **IPSec**

    IP Security. General IP Security mechanisms. IPSec Uses. Benefits of IPSec. IPSec services. Security Associations. SA Parameters. Security Policy Database. IPSec modes. Authentication Header. Encapsulated Security Payload. Encapsulating Security Payload.

24. **Kerberos**

    Needham-Schroeder protocol. Tickets. Authenticators. Kerberos protocol. Kerberos Realms. Kerberos Version 5.

25. **E-Cash**

    Blind signatures. Bitcoin. The block chain. Mining. Wallets. Security and attacks.

26. **Buffer Overflow**

    Hands-on exercise in C on buffer/stack overflow, showing how program code can be manipulated in order to elevate privileges and execute a program of your choice.

27. **Malware**

    History of malware. Types of malware. Viruses. Encryption and polymorphism. Worms. Zeus. Stuxnet. TDL-4. Flame. Mobile phone worms.

Topics covered in weekly readings

28. **Intrusion Detection**

    Intruders. Analysis Approaches. Host-Based Intrusion Detection. Network-Based Intrusion Detection. Distributed or Hybrid Intrusion Detection. Intrusion Detection Exchange Format. Honeypots. Snort.

29. **Firewalls and Intrusion Prevention Systems**

    Firewall Characteristics and Access Policy. Types of Firewalls. Firewall Basing. Firewall Location and Configurations. Intrusion Prevention Systems. Unified Threat Management Products.

30. **Software Security**

    Software Security Issues. Handling Program Input. Writing Safe Program Code. Interacting with the Operating System and Other Programs.

31. **Operating System Security**
    System Security Planning, Operating Systems Hardening, Application Security, Security Maintenance, Linux/UNIX Security, Windows Security, Virtualization Security.

32. **Windows Security**

    Windows Security Architecture. Windows Vulnerabilities. Windows Security Defenses. Browser Defenses. Cryptographic Services. Common Criteria.

33. **Dissecting Android Malware**

    Based on article "Dissecting Android Malware: Characterization and Evolution" by Yajin Zhou and Xuxian Jiang, presented at the IEEE Symposium on Security and Privacy

34. **The Nuts and Bolts of a Forum Spam Automator**

    Based on the article" The Nuts and Bolts of a Forum Spam Automator" by Youngsang Shin, Minaxi Gupta, Steven Myers

35. **Dark Clouds on the Horizon**

    Based on the article "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space" by Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber

36. **Pay-Per-Install Malware and the Underground Economy (PPI)**

    Based on the article "The Underground Economy of the Pay-Per-Install (PPI) Business" by Kevin Stevens, and "Measuring Pay-per-Install: The Commoditization of Malware Distribution" by Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson

37. **Car Security**

    Based on the article "Comprehensive Experimental Analyses of Automotive Attack Surfaces" by Stephen Checkoway, Damon McCoy, Brian Kantor,Danny Anderson, Hovav Shacham, and Stefan Savage

38. **Bluetooth security**

    Based on the article "Taming the Blue Beast: A Survey of Bluetooth-Based Threats" by John Dunning

Assignments and grading

There will be several quizzes, homeworks, one midterm and a final exam. All quizzes will be online, open-book, whereas the exams will be closed-book. The grading breakdown is the following:

Homeworks	30%
Quizzes	30%

Midterm exam	20%
Final exam	20%

Final grades are obtained by converting the numerical scores against the conversion table below:

F	D	C	C+	B-	B	B+	A-	A
< 60	60-68	69-73	74-78	79-83	84-87	88-91	92-94	95-100

Course Format

The course is blended and organized around the following pattern:
1. There will be an on-campus lecture every Wednesday based on a chapter from the textbook.
2. There will not be on-campus lectures on Mondays. Instead, students take an online quiz on a textbook chapter or a supplemental material.
3. The midterm and the final exam are based only on on-campus lectures. They will not cover the material included in the online quizzes.

Where and When to Turn in Assignments

The assignments must be submitted through Blackboard. I'll take ASCI text documents (like those prepared with NOTEPAD), MS Word documents, HTML pages, and PDF. Any other formats you should clear with me in advance.

Plagiarism

All academic work must be your own. Plagiarism, defined as copying or receiving materials from a source or sources and submitting this material as one's own without acknowledging the particular debts to the source (quotations, paraphrases, basic ideas), or otherwise representing the work of another as one's own, is never allowed. Collaboration, usually evidenced by unjustifiable similarity, is never permitted in individual assignments. Any submitted academic work may be subject to screening by software programs designed to detect evidence of plagiarism or collaboration.

The UIS Academic Integrity Policy (AIP) covers all academic misconduct, but three common violations are cheating, plagiarism, and facilitating violations of academic dishonesty. The UIS AIP is available at: http://www.uis.edu/academicintegrity/policy/

It is your responsibility to maintain the security of your computer accounts and your written work. Do not share passwords with anyone, nor write your password down where it may be seen by others. Do not change permissions to allow others to read your course directories and files. Do not walk away from a workstation without logging out. These are your responsibilities

Any student accused of a violation of academic integrity will receive an F for the course.

Attendance policy

Class attendance is required. Students are responsible for the content of all lectures they have missed. If a student is unable to attend class, he/she must contact me in advance. Course attendance could also affect your final grade.

No Extra Credit Work

Students sometimes ask for some extra credit work near the end of the semester in an attempt to bring up sagging grades. No extra credit work will be given to any student on an individual basis.

Incomplete work (I grade)

Under extraordinary circumstances, students may request a grade of "I" (incomplete). The granting of "I" grades is at the discretion of the instructor. Missing some lectures, quizzes, assignments or exams does not qualify for incomplete grade. For all missed assignments students will receive zero points.

Late Policy

If a student misses an exam or assignment, he/she will receive a zero for that portion of the grade, unless the student is ill (see the illness section below). There are no makeup exams or assignments**.**

Illness

In the event of an illness or other mishap, get proper documentation (e.g., medical certificate), but if you have grace days left, use them. If you need those days back later, give your documentation to me at that time.

Courtesy and disruption policy

It is expected that students will be courteous and mannerly in your dealings with your colleagues and the class staff. Students that engage in disruptions or interfere with the presentation of class content can be removed from the class. Conversation on mobile devises inside the classroom is prohibited. Cell phone and pager calls are considered as a class disruption.

Weather delays

If the university is closed on an assignment due date, it will be due by 2 p.m. on the first day the university reopens.

Students with disabilities

Reasonable accommodations are available for students who have a documented disability. Please notify the instructor during the first week of class of any accommodations needed for the course. Late notification

may cause the requested accommodations to be unavailable. All accommodations must be approved through the Office of Disability Services (ODS) in the Human Resources Building (HRB), Room 80, 217-206-6666.

Course Website

A Blackboard website will be setup for the course. The students are required to check the website regularly for lectures, assignments, and supplemental material. All quizzes must be taken online and homeworks must be submitted online.