**B O W I E S T A T E UN I V E R S I T Y**

*Department of Computer Science*

COSC 535: Information Privacy and Security

**Instructor:** Dr. Frank Xu

**Office:** Computer Science Building #216

**Office Hours:** TTH: 10:00-12:00 am& 1-2pm

**Phone: 2-**3965

**Email:** wxu@bowiestate.edu

**Classroom:** Computer science building # 309

**Class Times:** Wednesday 4:55-7:25PM

**COURSE DESCRIPTION**

Introduction to security and privacy issues associated with information systems. Technical, physical, and administrative methods of providing security. Identification and authentication. Encryption and management of encryption systems, including key protection and distribution. Cost/risk trade-offs. Privacy legislation and technical means of providing privacy.

**PREREQUISITE**

COSC 504 for graduate students

**PROGRAM OUTCOMES**

1. An ability to apply knowledge of computing and mathematics appropriate to the discipline
2. An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution
3. An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs
4. An ability to function effectively on teams to accomplish a common goal
5. An ability to use current techniques, skills, and tools necessary for computing practice.

**STUDENT EXPECTED OUTCOMES**

Through exams, homework assignments, team laboratory assignments, team projects and presentations, at the conclusion of this course, students will:

1. understand network border security, including firewalls, intrusion detection systems, virtual private networks, penetration testing and network security architecture (program outcomes: a-d, g-i);
2. develop the fundamental skills needed to analyze the internal and external security threats against a network (program outcomes: a-d, g,i);
3. know how to develop security policies that will protect an organization’s information (program outcomes: a-d, g, i);
4. know how to evaluate network and Internet security issues and design (program outcomes: a-d, g, i);
5. know how to implement successful network security policies and strategies (program outcomes: a-d, g, i);
6. know to expose system and network vulnerabilities and defend against them (program outcomes: a-d, g, i).

**STUDENT LEARNING OBJECTIVES (SLOs)**

1. To study network border security, including firewalls, intrusion detection systems, virtual private networks, penetration testing and network security architecture;
2. To develop the fundamental skills needed to analyze the internal and external security threats against a network;
3. To develop security policies that will protect an organization’s information;
4. To evaluate network and Internet security issues and design;
5. To implement successful network security policies and strategies;
6. To expose system and network vulnerabilities and defend against them.

**REQUIRED TEXTS**

* Pfleeger, Pfleeger & Margulies, Security in Computing, 5/E, 2015, ISBN-10:0134085043
* Michael Goodrich and Roberto Tamassia, Introduction to Computer Security, first edition，Pearson, 2011, ISBN-10: 0321512944.

**COURSE REQUIREMENTS AND EXPECTATIONS**

1. Research Presentation (for graduate students, individual/team based on enrollments)

You are required to pick one of the papers from the following conferences or journals for the research presentation. Note that **survey papers** are NOT encouraged for the research presentation. For your convenience, I have included the two links to the list of conferences and journals. <http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm>.

http://icsd.i2r.a-star.edu.sg/staff/jianying/conference-ranking.html

TABLE I. Example of Security-related Conferences

|  |  |  |
| --- | --- | --- |
| Rank 1 | [S&P](http://www.ieee-security.org/TC/SP-Index.html) (Oakland) | IEEE Symposium on Security and Privacy |
| [CCS](http://www.acm.org/sigs/sigsac/ccs/) | ACM Conference on Computer and Communications Security |
| [Crypto](http://www.iacr.org/conferences/) | International Cryptology Conference |
| [Eurocrypt](http://www.iacr.org/conferences/) | European Cryptology Conference |
| [Security](https://www.usenix.org/conferences/byname/108) | Usenix Security Symposium |
| [NDSS](http://www.isoc.org/isoc/conferences/ndss/) | ISOC Network and Distributed System Security Symposium |
| Rank 2 | [ESORICS](http://www.laas.fr/~esorics/) | European Symposium on Research in Computer Security |
| [RAID](http://www.raid-symposium.org/) | International Symposium on Recent Advances in Intrusion Detection |
| [ACSAC](http://www.acsac.org/) | [Annual Computer Security Applications Conference](http://www.acsac.org/2004/welcome.html) |
| [DSN](http://www.dsn.org/) | The International Conference on Dependable Systems and Networks |
| [CSF](http://www.ieee-security.org/CSFWweb/) (CSFW) | IEEE Computer Security Foundations Symposium.  Supersedes CSFW (Computer Security Foundations Workshop) |
| [TCC](http://www.wisdom.weizmann.ac.il/~tcc/) | Theory of Cryptography Conference |
| [Asiacrypt](http://www.iacr.org/conferences/) | International Conference on the Theory and Application of Cryptology and Information Security |
| [IMC](http://www.sigcomm.org/events/imc-conference) | Internet Measurement Conference |
| [PETS](http://petsymposium.org/) | Privacy Enhancing Technologies Symposium |

PRESENTATION GUIDELINES

Plan to give a 15-minute over-head presentation, with time for questions and discussion. Presentations should be self-contained, and should be clear and precise. Briefly introduce the topic including any background information, describe the investigation, development, or experimentation that was conducted, and provide any demonstrations developed as part of the project, or describe the results of the investigation or experimentation. The following format is required:

1. Title. Name of the project and all the team members.
2. Outline. Summarize the full presentation.
3. Introduction. Introduce the purpose and goals of the project. Provide any background material necessary to understand the presentation.
4. Investigation, development, or experimentation conducted. Describe the actual work performed during the project.
5. Results. Show any demonstrations developed or results achieved during the project.
6. Conclusion
7. References
8. Questions and discussion
9. Research Project (for graduate students, individual/team based on enrollments)

You are required to produce a team research project. You will be working with other class members as part of a team. Projects must culminate with a *presentation* for the class and the submission of a *final report*. All projects must be approved by the instructor. The format of the presentation and final report are listed above.

1. Lab Projects (**ONLY** for undergraduate student, individual/team based on enrollments)

Pick up one of the lab from <http://www.cis.syr.edu/~wedu/seed/labs.html>. Notes you should not choose any labs have been covered or will be covered in this class. You need to submit a video to demonstrate you work.

1. Labs (All students, individual, not all labs will be covered)

|  |  |  |  |
| --- | --- | --- | --- |
| **Types** | **Labs** | **Suggested Time (week)** | **Chapters** |
| **Vulnerability and Attack**  **(Linux-based)** | Buffer Overflow Vulnerability | 1 | 3 |
| Return-to-libc Attack | 1 | 3 |
| Format String Vulnerability | 1 | 3 |
| Race Condition Vulnerability | 1 | 3 |
| Set-UID Program Vulnerability | 1 | 3 |
| Chroot Sandbox Vulnerability | 1 | 12 |
| Cross-Site Request Forgery Attack | 1 | 7 |
| Cross-Site Scripting Attack | 1 | 7 |
| SQL Injection Attack | 1 | 7 |
| ClickJacking Attack | 1 | 7 |
| TCP/IP Attacks | 2 | 5 |
| DNS Pharming Attacks | 2 | 6 |
| **Exploration Labs**  **(Linux-based)** | Pack Sniffing & Spoofing | 1 | 5 |
| Pluggable Authentication Module | 1 | 3 |
| Web Access Control | 1 | 7 |
| SYN Cookie | 1 | 5 |
| Linux Capability | 1 | 3 |
| Secret-Key Encryption | 1 | 8 |
| One-Way Hash Function | 1 | 8 |
| Public-Key Infrastructure | 1 | 8 |
| **Design and Implementation** | Virtual Private Network (Linux) | 4 | 6 |
| IPSec (Minix) | 4 | 6 |
| Firewall (Linux) | 2 | 6 |
| Firewall (Minix) | 2 | 6 |
| Role-Based Access Control (Minix) | 4 | 9 |
| Capability-Based Access Control (Minix) | 3 | 3 |
| Encrypted File System (Minix) | 4 | 9 |
| Address Space Randomization (Minix) | 2 | - |
| Set-RandomUID Sandbox (Minix) | 1 | 13 |

**Grading Policies**

|  |  |
| --- | --- |
| **Item** | **Points** |
| Lab/Projects/homework/Quizzes | 100 |
| Midterm | 100 |
| Final | 100 |
| Total | 300 |

|  |  |  |
| --- | --- | --- |
| **Grade** | **Grade Scale** | **Points** |
| A | 90% | 270+ |
| B | 80% | 240+ |
| C | 70% | 210+ |
| F | 59% and below | below 210 |

TABLE II. Course Outline

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Topics** | **Chapter**  **Readings** | **Exams** |
| **1** | Introduction | Chapter 1 |  |
| **2** | Toolbox: authentication, access control, and cryptography | Chapter 2 |  |
| **3** | Programs and programming | Chapter 3 |  |
| **4, 5** | Web-User side | Chapter 4 |  |
| **6, 7** | Operating systems | Chapter 5 |  |
| **8** | Midterm review |  | Mid-term Exam |
| **9** | Networks | Chapter 6 |  |
| **10** | Database | Chapter 7 |  |
| **11** | Privacy | Chapter 9 |  |
| **12** | Management and Incidents | Chapter 10 |  |
| **13** | Legal Issues and Ethics | Chapter 11 |  |
| **14** | Final Review |  | Final Exam |

**Course Policies:**

1. Homework/Lab is due by the beginning of the next class.
2. Late homework will be given zero.
3. You cannot start a new assignment until the previous assignment has been received by the instructor.
4. No make-up quizzes/exams will be allowed without prior arrangements being made.
5. Do not ask questions such as "How do you solve Problem X?" Explain what you have done and ask a specific question in that context.
6. Be seated, quiet, and ready to learn when the class time begins. Do not speak when someone else is speaking.
7. Do not eat or drink in class because the sights, smells, and noises can be distracting to others. Be considerate and respectful of everyone.
8. To appeal a grade, send an e-mail to your instructor's e-mail address within two weeks of the grade having been received. Overdue appeals will not be considered.
9. All noise-make devices, such as cellular phones, pagers, CD players, radios, and similar devices are prohibited in the classroom and laboratory facilities.
10. Calculators and computers are prohibited during examinations and quizzes, unless specified.
11. Reasonable laptop-size computers may be used in lecture for the purpose of taking notes.

**Important Reminders from the Bowie State University Administration**

Students who have a disability and want accommodations should report immediately to **Disability Support Services** (DSS), located in Room 079 in Thurgood Marshall Library or call Dr. Michael S. Hughes, DSS Coordinator, at 301-860-4067.

Please take your **English Proficiency Examination** as early as possible! After completing ENGL 101 and ENGL 102, students must take and successfully pass the Bowie State University English Proficiency Examination. Transfer students who completed their English composition requirements at another university should take the English Proficiency Examination during their first semester of enrollment at the University.

In case of **inclement weather conditions**, call the following number regarding cancellations:

(301) 860-4000 or check online at www.bowiestate.edu.

Students who are not registered for this course will not receive a grade.