University of Washington

i310 – CyberSecurity and Information Assurance

Winter, 2016

Instructor: James Farricker (james.t.farricker@boeing.com best email)

Course Objectives

Students will:

- Understand and apply the information perspective
  - Appreciate the concepts of information privacy and accountability
  - Understand the relationship between people and IA practices and technology
- Understand the underlying technologies associated with IA
  - Achieve a working understanding of cryptography by studying theory and using it to communicate
  - Understand digital signatures and certificates
  - Develop a knowledge of common attack vectors and their mitigations
  - Understand common technology terms and concepts that are encountered in the field of IA
- Analyze the information assurance (IA) context
  - Demonstrate understanding of threats, vulnerabilities, strategic countermeasures in a variety of contexts
  - Describe the system services and strategies that implement IA
  - Understand the life cycle for IA in an organizational context
- Apply the principles of management
  - Understand the role and responsibilities of a CISO (Chief Information Security Officer)
  - Understand the role of risk management in IA decision making
  - Understand the human factors affecting the validity of IA policy and plans
  - Address legal and ethical issues related to IA
- Get excited about information assurance and cyber-security

Course Administration

Attendance

Students are expected to attend all classes unless a sufficient excuse is provided or prior arrangements are made with the instructor.

Textbook

Bishop, M. (2012). Computer Security.
ISBN: 978-0321712332

Papers

Recent papers on key topics will be assigned and either handed out in class or linked to online.

Time

TBD

Participation

As stated in the syllabus, class participation is important. Please read the assignments ***before*** class. Discussions will focus on that week's topics.

Assignments & Late Policy

There will be a 10% late penalty per day for late assignments. Assignments over a week late not accepted, unless absence approved in advance.

Scholastic Honesty

Scholastic dishonesty is broadly any act which violates the rights of other students in the execution and evaluation of their work, or which involves misrepresentations of the work of another as one's own. You are expected to do your own work. In addition, all students will be expected to sign and date the policy statement at the end of the syllabus.

Also students are expected to adhere to the highest standards of ethical behavior and sign the computer lab use policy at the end of the syllabus the first week of class.

Grading

Participation (current events, class discussion, reading)	10%
Quizzes	15%
Midterm Exam	25%
Labs (lab deliverables, lab execution)	20%
Final Exam	30%
	100%

Course Progression

The following is the class progression covering the 10 weeks for the course. The class will meet three times a week, twice in lecture for 1 hour and 50 minutes and once in lab for 50 minutes. Every class will start with a 10-20 minute review of current events. This will familiarize students with the IA and CS happenings in the world and provide real world to anchor what they will be learning in lecture.

Week 1: Overview

HW	Read Bishop Chapters 1-2, Handout
L1	Syllabus, Policies, Overview of Course
L2	Terminology, History, Significance
Lab	Source of Information on the Internet

Week 2: The Basics

HW	Read Bishop Chps 4,5,7
L1	Evolution of Security
L2	IA Pillars, Topic Areas in Cyber Sec
Lab	Sec Perim Arch Case/LAN Turtle ?

Week 3: Crypto, Key Mgmt, Authentication

HW	Bishop Chaps 9-11 (L1), 12,14 (L2)
L1	Encryption, Hashing, Key Mgmt, PKI
L2	Authentication: Biometrics, multi-factor
Lab	Network frame/packet capture Prot analysis/flows *http: man in middle attack*

Week 4: Web Applications

HW	Read Bishop 14.6, Handout
L1	Web Browser Vulnerabilities
L2	Intro to Pen Testing (M. Nishimoto)
Lab	Intro Kali Linux – tools.

Week 5: Malware & Social Engineering

HW	Bishop Ch 22, Stuxnet, Mitnick URLs
L1	Malware and Botnets;
L2	Social Engineering
Lab	Kristina Lab: Attack Web Browser MyDoom, Conficker (read - URLs).

Week 6: Sec Code Dev, Net Enabled

HW	Read Bishop Chapter 18, Handouts
L1	**S/W Assurance MIDTERM Rev**
L2	**MIDTERM EXAM**
Lab	**MIDTERM EXAM**

Week 7: Networks & Internet Infrastructure

HW	Read Bishop Chps 15,25,26, Handout
L1	Netcentric Defenses, correlation tools
L2	Wireless Security & SIGINT
Lab	ACL's/Firewalls Wireless Net Security Case

Week 8: Policy and Management

HW	Bishop Chaps 21,23-24, Handout
L1	IA in the Enterprise
L2	Setting up governance model
Lab	Cloud Computing (Def in Depth challenge) ***or WiFi Pineapple Lab***

Week 9: Jobs in Computer Security

HW	Read Bishop Chaps 27-28, Handout
L1	Real World (NIST, RMF, HIPA)
L2	Certifications
Lab	Red team/Blue team challenge Cyber Sec/IA Skills Assessment Case

Week 10: Social Networking & Privacy

HW	Bishop Chapter 29, Handout
L1	Risks Social Networking, **Final Rev**
L2	**Final Exam**
Lab	**Final Exam**

Week 1 – Overview

HW Bishop (Chapters 1-2), Handout – Intro to Cyber Security
L1 Syllabus, Policies, Overview of Course
L2 Terminology, History, Significance
Lab Source of Information on the Internet

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Understand the goals of the course
2. Understand the policies and practices at the University of Washington regarding computer security
3. Describe the progression of the course and milestones
4. Comprehend the responsibilities of a cyber-security professional
5. Understand the ethical ramifications of negligent or malicious computer use
6. Explain the proper computer lab use policy
7. Demonstrate that they know the grading, attendance, participation and late day policies
8. Explain the key deliverables for the course

Lab and Practice – After completing this lab, students should be able to:

1. Locate reliable sources of information on computer security online
2. Keep up to date on developments in the fields of information assurance and computer security
3. Learn and teach themselves keywords and concepts on their own
4. Be able to find various vulnerability bulletin boards
5. Explain how to find out more information on unfamiliar terms
6. Identify credible sources of knowledge for information assurance and cyber security topics

Lab Deliverable: write-up of approximately ½ to 1 page where student will pick resource/web site indicating:

Basis Site/resource was chosen	***(20%)***
Basic related technical area of IA/CyberSec explained	***(40%)***
Explain how resource will enhance your understanding of IA/CyberSecurity	***(40%)***

Additional information on lab (and other labs will be emailed as required) and TA will post on Canvas

Week 2 – The Basics

HW Bishop (Chapters 4,5,7) & Handouts (Pillars of IA, Stuxnet)
L1 Evolution of Security
L2 Topic Areas in Security Profession
Lab ***Review:*** Enterprise Security Perimeter Architecture
Explore Common Vulnerabilities and Exposures (CVE) *http://cve.mitre.org/*

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Identify key points of evolution in the security field
2. Understand how the term hacking has evolved in popular culture
3. Explain the differences between a hacker, cracker, script-kiddie, white hat, grey hat, and black hat
4. Describe the key areas of computer security
5. Explain the difference between information assurance and cyber-security
6. Differentiate between forensics, incident response, policy, pen-testing, vulnerability assessment and exploit development.
7. Categorize various threats and the nature of their risks
8. Differentiate between network centric and data centric security methods.
9. Demonstrate an understanding of a basic threat model
10. Describe the benefits and limitations of data protection for "data at rest" and for "data in motion"
11. Understand risk management, security policy exceptions and technical; risk cube (likelihood & consequence)

Lab and Practice – After completing this lab, students should be able to:

1. Be able to navigate to and search through the CVE list
2. Explain the CVE severity rating system
3. Articulate the importance of the CVE system for IA professionals
4. Effectively research key terms to determine the nature of the vulnerability detailed in the report
5. Describe the common components and security strategies/methods utilized in home, business and enterprise security perimeters.
6. Understand the challenges of protecting the information resources of a business/organization.

Lab Deliverable: write-up of approximately ½ to 1 page demonstrating understanding of:

Basic Similarities/Diff Home/Bus/Ent Sec Strategies (40%)
Explain how Defense in Depth applied against lab use cases (30%)
Based on lab/lecture concepts what your basic arch recomm for each of the scenarios (30%)

Week 3 – Cryptography & Authentication

HW Bishop (Chps 9,10,11 Crypto Reading), (Chps 12,14 Authentication/Identity Reading), Handout
L1 Intro to Cryptography, encryption and key management
D/H Encryption & Hashing
L2 Authentication and Identity
Lab WireShark – capturing/analyzing data traffic (using a protocol analyzer)
Crypto and Authentication Use Case (Company/factory wireless LANs)

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Retell the history of the Caeser Cipher and Enigma machine
2. Describe how Diffie-Hellman key exchange works at a high level
3. Identify where DH key exchange is used in IT
4. Explain the difference between hashing and encryption
5. Demonstrate an understanding of what DES and AES are
6. Explain how both algorithms have come into common use
7. Describe how hashing algorithms work at a high level
8. Explain the purpose of hashing algorithms in IT
9. Explain key management and pki
10. Understand and describe the business and regulatory implications of crypto in a global environment.
11. Describe the requirement and security implications of multi-factor authentication
12. Differentiate cyber security related advantages and disadvantages associated with password based security, and use of biometrics in authentication.

Lab and Practice – After completing this lab, students should be able to:

1. Demonstrate understanding of key management and pki
2. Describe what makes a good hashing algorithm
3. Demonstrate understanding of the business and regulatory implications of crypto in a global environment.
4. Demonstrate use of encryption, PKI, and multi-factor authentication in multiple use case environments.
5. Demonstrate ability to capture Ethernet frames and TCP/IP packets
6. Describe application flows and dependencies
7. Understand TCP/UDP ports and how used in firewall/IDS components

***Lab details/deliverables will be emailed*.**

Week 4 – Web Applications

HW Bishop (Chapter 14.6) Handout
L1 Components of a Web Application
L2 Web App Attack Vectors
Lab Access-lists, IP address, TCP port filtering (http)
http: man in middle attack, ***Port Scanning***

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain what a web application is and give several examples of commonly used web applications
2. Identify the key parts of a web application
3. Explain the architecture of a generic PHP based web application and what happens behind the scenes
4. Show an example of a web application and describe how the components work together
5. Describe common attack vectors against web applications
6. Look at an example web application and point out possible attack vectors
7. List the OWASP Top 10
8. List defenses and common practices to mitigate the threats in the OWASP Top 10
9. Explain common best practices that mitigate web application vulnerabilities
10. Describe the procedure and principles of responsible disclosure

Lab and Practice – After completing this lab, students should be able to:

1. Examine a web application and point out possible vulnerabilities
2. Analyze a web application for relevant OWASP concerns
3. Perform a superficial audit of a web application
4. Analyze the impact severity of the possible attacks against the web app
5. Format the audit into a report for the developer of the web application
6. Understand vulnerabilities of HTTP (sending in clear)
7. Apply concepts from prev week lab (crypto) to protect web traffic
8. Apply principles of port scanning to improving security computing environments.

Lab details/deliverables will be emailed

Week 5 – Malware and Social Engineering

HW Bishop (Chapter 22) & Mitnick Readings, NSA Handout/Guidance on Defense against Malware on Removable Media
L1 Malware and Botnets
L2 Social Engineering
Lab Reversing & Malware Analysis/Training
Basic Malware Analysis
Client VPN – Malware Case Study

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain the threat malware poses to the average user
2. Explain the threat malware poses to an organization or country
3. Describe the commodification of malware production, spreading, data harvesting, and commerce
4. Understand the evolving uses of malware by crime groups
5. Describe common botnet command and control configurations
6. Explain defenses against malware in an organizational context
7. Describe how honeypots work
8. Explain the mechanics of sink-holing and how sinkholes can be used to both fight and examine malware
9. Analyze Stuxnet, it's development, target, threat vector, and describe its discovery and analysis
10. Explain the implications of nation-state sponsored cyber warfare
11. Describe MyDoom, & Conficker
12. Understand the aspects of social engineering and how it sits within the information assurance and computer security field
13. Describe several key types of social engineering
14. Explain the threat social engineering poses for organizations
15. Illustrate the relationship between social engineering and technical exploitation

Lab and Practice – After completing this lab, students should be able to:

1. Explain the evolution of the term "Hacker"
2. Describe the role hackers play in our society both positive and negative
3. Describe the changes to the field of computer security that have come as a result of the rise and change in hacker culture
4. Make educated predictions as to the future of hacking
5. Relate developments in hacking to changes in public policy and business operations.

Lab details/deliverables will be emailed

Week 6 – Writing Secure Code

HW Bishop (Chp 18), Handouts
L1 **MIDTERM**
L2 Application Defenses
Lab S/W Assurance Case
Dbase access controls/rights

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain common secure coding techniques
2. Describe commonly used defenses integrated with tools such as GCC and the JVM
3. List the top vulnerabilities in application development that come as a result of poor coding practices
4. Outline proper best practices to ensure vulnerabilities aren't introduced while developing applications
5. Effectively take a test
6. Understand software assurance design guidelines
7. Explain how software scanning tools are utilized to ensure code validation
8. Describe different S/W scanning approaches (static/dynamic) and implications to S/W developers and integrators.

Lab and Practice – After completing this lab, students should be able to:

1. Complete the basic challenges on hackthissite.org
2. Explain the benefits of practice in learning cyber-security techniques
3. Describe common vulnerabilities that come up as a result of poor coding practices
4. Demonstrate a proficiency in researching vulnerabilities online
5. Show hands on experience in exploiting development mistakes
6. Describe S/W scanning approaches (static/dynamic)
7. Explain how software scanning tools are utilized to ensure code validation

Lab details/deliverables will be emailed

Week 7 – Networks

HW Bishop (Chps 15, 25,26), Handout
L1 Network Based Defenses, Intrusion Detection
L2 Wireless Security and SIGINT
Lab Wireless security
Wireless Network Security case

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Describe the various components of a network and security perimeter
2. Explain how DHCP, DNS, routers, switches, and firewalls all function to provide connectivity on a network
3. Identify possible vulnerabilities in a network
4. Describe how DNS can be exploited to provide an advantage to hackers
5. Explain the fundamentals of ARP spoofing and how that can be used to sniff people's traffic
6. Explain the function of intrusion detection systems/appliances
7. Explain the impact of big name worms/viruses and how they have changed the security scene and business practices at organizations dependent upon Internet based infrastructure.
8. Describe the basic principles of SIGINT.
9. Explain security vulnerabilities and techniques to mitigate in a wireless LAN (IEEE 802.11) environment.
10. Describe how parts of the MAC layer and network layer (OSI layers) are used in cyber security protection systems/methods.
11. Understand role of 802.1X in protecting business/organization networks..

Lab and Practice – After completing this lab, students should be able to:

1. Describe the components and technologies utilized to support enterprise based security perimeters
2. Explain vulnerabilities of using wireless based connectivity.
3. Describe techniques utilized in wireless LANs that help mitigate these vulnerabilities.
4. Understand network centric based cyber security tools
5. Demonstrate knowledge of mobile/wireless vulnerabilities, methods to enhance security.
6. Describe wireless protection/security methodologies including WEP, WPA/WPA2, X.509 Digital Certificates for authentication..

Lab details/deliverables will be emailed

Week 8 – Policy and Management

HW Bishop Chaps 23-24, Handout
L1 IA in the Enterprise
L2 IA in the Daily Life
Lab Daily Walkthrough
Setting Up Governance Model

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Explain the role of information assurance in an enterprise environment
2. Illustrate some common functions a security team would play in an enterprise environment
3. Describe several common organizational policies related to IA such as password strength requirements and sensitive data disposal techniques
4. Describe the roll of a CISO and how that differs from the CIO
5. Identify where information assurance risks exist in their everyday lives
6. Explain the dangers of identity theft and personal sensitive data leakage
7. Perform a self audit to determine what information risks the student is exposing themselves to based on their current habits
8. Demonstrate and understanding of how to mitigate non-adversarial threats such as hard drive failure, fire, and power outages
9. Explain what RAID is and how it works
10. Illustrate common data replication techniques used by cloud based providers
11. Give some examples where non-adversarial threats have cause damage and how the companies dealt with those damages
12. Describe the key attributes of an effective governance model to successfully implement cyber security protection mechanisms in an organization.

Lab and Practice – After completing this lab, students should be able to:

1. Do a mental walkthrough of their daily lives to identify security risks
2. Identify and prioritize those risk so they can be dealt with responsibly
3. Demonstrate an understanding of weighing daily risks and their mitigation techniques
4. Develop a plan to secure one's personal information and ensure privacy
5. Implement and regularly audit the plan to discover possible weaknesses in the self guided policy
6. Explain the benefits and significance of an effective governance model to implement cyber security controls and protection mechanisms

Lab details/deliverables will be emailed

Week 9 – Professions in Computer Security

HW Bishop Chps 27-28 Reading, Handout
L1 Out in the Real World
L2 Certifications
Lab Red team/Blue team challenge
Cyber Security/IA Skills Assessment Lab

Learning Objectives

Theory – After L1 and L2, students should be able to:

1. Demonstrate an ability to find jobs in the computer security field
2. Identify common skills necessary to be competitive in the computer security field
3. Describe the merits and focuses of various common security related certifications
4. Differentiate between the management and policy focused certifications and the technical centric ones
5. Understand requirements specific to the government sector such as clearances
6. Design a path to their security related dream job
7. Explain how cyber forensics within law enforcement works and how it is different from forensics in a corporate environment
8. Make an educated prediction about changes in the job market
9. Present current and future qualifications to best increase the chances of getting ideal job placement

Lab and Practice – After completing this lab, students should be able to:

1. Identify large employers of computer security professionals
2. Describe several industry certifications
3. Explain the various requirements for each certification
4. Analyze and predict where the computer security profession is headed in the next few years
5. Describe technical skills required to succeed in Cyber Security/IA industry opportunities
6. Demonstrate knowledge of system/component vulnerabilities by attempting to exploit or protect networks and systems from denial of services, disrupted communications or other exploits which would permit unauthorized access/change to lab computing/networking resources.

Lab details/deliverables will be emailed

Week 10 – Social Networking and Privacy

HW Bishop Chps 29-30 Reading, Handout
L1 Risks with Social Networking
L2 Review
Lab Application of STRIDE. Use Case using STRIDE for threat modeling and classifying computer security threats

Learning Objectives:

Theory – After L1 and L2, students should be able to:

1. Identify risks associated with using social networking platforms
2. Describe best practices for ensuring privacy while using social networking platforms
3. Illustrate the dangers of cookies and how they can compromise an online identify or track a user's habits
4. Explain how the Tor network and onion routing works
5. Describe the benefits of using a VPN or SSH tunnel for browsing
6. Outline the utility and risk with using proxies
7. Describe what a SOCKS proxy is
8. Explain common anonymity practices
9. Describe how torrent and P2P networks work
10. Outline best practices for securing torrent and p2p usage
11. Explain what they have learned in this class

Lab and Practice – After completing this lab, students should be able to:

1. Properly manage access to the information on their social networking profiles
2. Explain the importance of securing their social networking profiles and controlling their online presence
3. Identify possible information leaks in the configuration of social networking sites
4. Set up the Tor Browser Bundle
5. Demonstrate common anonymous browsing techniques
6. Demonstrate use of STRIDE for threat modeling and classifying computer security threats

Readings

Stuxnet

http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

Mitnick

http://www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story/

MyDoom

http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/
http://www.wired.com/threatlevel/2009/07/mydoom/

Conficker

http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/?single_page=true

Please read the following and sign the document:

Info 310 Computer Security, Information Assurance and Ethics IA Lab Use Policy:

1. The following University of Washington lab use policy will be in effect, which can be found at: http://www.ischool.washington.edu/technology/labs/policies.aspx

2. The University of Washington acceptable computer use policy will be in effect, which can be found at: http://www.washington.edu/computing/rules/

3. The Info 300 General Responsibilities for All Students policy will be in effect, which can be found on the first page of this syllabus and on the following web site:

4. Due to the special nature of the Lab Exercises for this course certain additions to the above policies will be in effect, they are the following:

- Every experiment run in conjunction with this course will have certain rules and regulations regarding its conduct. These will be explained when the assignments are given and students are expected to comply with any additional restrictions.
- To the extent that lab computers are used to stage attacks under controlled circumstances, they will be physically disconnected from all external networks. All student users of this lab must maintain this lack of connection and must verify this lack of connection (with instructor help) before running any malicious code or exploit.
- Students may be allowed to attempt to run harmful software and obtain root access on lab computers isolated from the network, as long as the students in question agree to fix any problems they cause (e.g. hardware damaging code).
- Security flaws and other problems in this lab should be pointed out immediately to the lab instructor first before calling the help desk.
- Any student running an exploit in connection with assignments in this class must file an Exploit Approval form with the instructor, before running any malicious code or attempting any exploit on any lab computer.
- Students are responsible for the consequences of any actions they take without the knowledge of the lab instructor.

I, _____, hereby certify that I have read and understand this policy and the relevant University of Washington policies referenced above regarding computer lab use and will abide by them.

Signature _____

Printed Name _____

Student ID No. _____

Dated _____

Code of Conduct

The following code of conduct has been adopted for this course:

General responsibilities for all students

Students are trusted with access to the practices, procedures and technologies used to attack and protect valuable information assets and systems. This trust requires an uncompromising commitment to satisfying the highest moral and ethical standards. Adherence to all laws, rules and regulations applicable to the field and practice of information security is critical. This requires more than simple obedience to the law. We expect that students trained by UW will demonstrate sound ethics, honesty and fairness in providing security products and services. UW expects each student to assume a sense of personal responsibility for assuring the compliance of his or her own behavior and those of their fellow students. The Code of Conduct represents a "zero tolerance" policy. All students enrolled in this course are expected to conduct their activities in a manner that satisfies the highest of ethical standards. Each student must:

- ✓ Conduct activities in accordance with high ethical and moral standards
- ✓ Conduct all activities in accordance with the academic integrity standards posted on the UHM web site
- ✓ Be aware of, and abide by, the laws of the United States, the individual States, foreign countries and other jurisdictions in which the student may conduct studies, projects, research or other activities
- ✓ Adhere to the spirit of the law as well as its substance
- ✓ Always act with personal integrity based on principles of sound judgment
- ✓ Neither condone nor ignore any illegal or unethical acts for any reason

Students should be aware that they may be held personally liable for any improper or illegal acts committed during the course of their education, and that "ignorance of the law" is not a defense. Students may be subject to civil penalties, such as fines, or regulatory sanctions, including suspension or expulsion. Potential penalties for illegal acts under federal sentencing guidelines are severe and may include imprisonment and substantial monetary fines. Existing federal and state laws, as well as the laws of foreign jurisdictions, may impose civil money penalties, permit the issuance of cease and desist orders, or have other consequences.

It is imperative that UW and its students conduct the University's academic activities in accordance with the highest possible ethical and legal standards. Every student is responsible for ensuring that his or her personal conduct is above reproach. Violations of the standards described in this Code of Conduct should be made known immediately to the instructor. UW takes these ethical obligations very seriously. Violations will not be tolerated and will result in disciplinary action appropriate to the violation.