CityUniversity of Seattle

Syllabus

SCHOOL OF TECHNOLOGY AND COMPUTING

ISEC 515: Privacy and Open Systems

3 Credits
Effective: Fall 2019

Access to the Internet is required.
All written assignments must be in Microsoft-Word-compatible formats.
See the library's APA Style Guide tutorial for a list of resources that can help you use APA style.

FACULTY

Faculty Name: Dr. Billy Chestnut

Email: Chestnutbilly@cityu.edu

Phone or Skype: 540-623-0914

Office Hours and Response Time: Office Hours will be from 5pm - 6pm (Eastern Time) via telephone. Please contact me for emergencies only. Email is the preferred method of communications. I will respond within 24 hours. I will grade assignments within 3 business days after the due date.

COURSE DESCRIPTION

In the highly connected world in which we live, our personal information, classified data, and communications are increasingly vulnerable to interception, attack, and abuses ranging from identity theft to restrictions on our freedoms. In this environment, it is essential to address issues of privacy and anonymity. This course explores privacy policy, privacy engineering, cryptology, and the use of open systems designed to protect privacy. Students will leave this course with an understanding of how to ensure their organizations support privacy requirements and how to maintain privacy in communications.

COURSE RESOURCES

Required and recommended resources to complete coursework and assignments are available from the Course Document Lookup.

CityU online resources are used. No purchase is required.
Textbook

[DENN14] Dennedy, M., Fox, J., & Finneran, T. R. (2014). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Apress. (ISBN: 9781430263555)

[LOSHa13] Loshin, P. (2013). *Simple Steps to Data Encryption: A Practical Guide to Secure Computing*. Syngress Publishing. (ISBN: 9780124114838)

[LOSHb13] Loshin, P. (2013). *Practical Anonymity: Hiding in Plain Sight Online*. Syngress Publishing. (ISBN: 9780124104044)

Module 1

[LEAC15] Leach, Hannah. It's Not YOUR Data, Didn't You Know? Cities of the Future. 30 November 2015. https://citiesofthefuture.eu/its-not-your-data-didn-t-you-know-93cc2fcc76d8

Module 10

[SURV18] Surveillance Self-Defense. (1018). The Problem with Mobile Phones. Retrieved from https://ssd.eff.org/en/module/problem-mobile-phones

CITYU LEARNING GOALS

This course supports the following City University learning goals:

- Professional competency and professional identity
- Diverse and global perspectives

COURSE OUTCOMES

In this course, learners:

- Explore how encryption is used to protect privacy and support authentication.
- Implement and use tools to protect privacy and anonymity.
- Conduct assessments of privacy systems, processes, procedures, awareness, and readiness.
- Develop and apply a privacy policy based on applicable privacy laws and regulations.
- Recognize and protect information which needs to be private or classified.

CORE CONCEPTS, KNOWLEDGE, AND SKILLS

- Analyze the impact of enterprise sectors on the development of privacy policies.
- Assess quantitative value from privacy engineering.
- Assess the different forms of privacy, such as behavioral privacy, decisional privacy, and physical privacy.
- Assess the implications of posting a key to a key server.
- Assess what is required for a 'good' policy.
- Build a communication and training plan for privacy awareness and readiness.
- Compare and contrast clear signed, detached, and attached signatures.
- Compare and contrast privacy, confidentiality, and security.
- Compare and contrast the two types of Personal Information Services.
- Compare privacy laws and privacy frameworks.
- Compare the challenges of privacy engineering to the challenges of Operations Research.
- Compare the domains of different privacy frameworks.
- Compare valuation models for assessing privacy values.
- Conduct a privacy awareness and readiness assessment.
- Consider the context in which a privacy initiative will operate.
- Correlate privacy awareness and readiness to risk management.
- Create an annotated list of what should be included in a privacy policy in a specific instance.
- Debate how privacy can be maintained with a Bring Your Own Device (BYOD) program.
- Decrypt and verify a message using a public key.
- Define anonymity.
- Define Data Governance.
- Define Personally Identifiable Information.
- Describe and discuss Data-Centric and Person-Centric processing.
- Describe forensic analysis of mobile phones.
- Describe how privacy policies provide the foundational layer of privacy engineering and use-case requirements.
- Describe how privacy requirements are developed.
- Describe how privacy requirements are reviewed throughout the engineering lifecycle.
- Describe how to de-identify or anonymize personal information.
- Describe methods for assigning value to data.
- Describe public Key Encryption.
- Describe the concept of symmetric encryption.
- Describe the effects of privacy policy on qualitative value from improved efficacy of data system flow and customer value.
- Describe the use and limitations of proxy servers to access otherwise unavailable servers.

- Develop an understanding of how privacy is engineered into systems.
- Develop privacy requirement use cases.
- Diagram how a man-in-the-middle attack works.
- Diagram how TOR functions.
- Differentiate between meta-data and data.
- Discuss Fair Information Processing Principles.
- Discuss five evolutionary stages of information sharing and the evolution of privacy and security concerns.
- Discuss full disc encryption.
- Discuss how GPS is used for tracking.
- Discuss how ISO 2700X supports privacy.
- Discuss how service level requirements impact privacy policies.
- Discuss privacy issues in the cloud.
- Discuss the benefits of a data governance program.
- Discuss the benefits of having diverse users of TOR
- Discuss what privacy engineers should take responsibility for and the benefits they should provide to individuals, businesses, and government.
- Encrypt a message using public key encryption.
- Encrypt and decrypt data using symmetric encryption.
- Encrypt and sign a file for distribution using a public key.
- Enumerate and discuss the Generally Accepted Privacy Principles (GAPP)
- Establish goals and build an operational plan for Privacy Awareness and Readiness.
- Establish the conditions for an effective privacy awareness and readiness program.
- Evaluate how changes in the delivery of services affect privacy requirements.
- Evaluate how internal and external service requirements impact on privacy policies.
- Evaluate how privacy is protected in physical environments.
- Evaluate how the user experience affects privacy requirements.
- Evaluate the importance of using strong pass phrases.
- Evaluate the issues involved with using public key servers.
- Evaluate the issues of having a pass key stored in RAM.
- Evaluate the merits of using Open Source code for encryption.
- Evaluate the merits of using the Command Line Interface to learn encryption.
- Evaluate the placement of Quality Assurance in the privacy development structure.
- Evaluate the requirements to develop a global privacy policy.
- Evaluate the risk of introducing privacy issues during the Quality Assurance process.
- Evaluate the risks of using and exchanging keys in different circumstances.
- Evaluate the tradeoffs in determining key length.
- Examine how burner phones are used to aid anonymity.
- Examine how use cases change with different classifications of data.
- Examine how use cases provide a tool for requirements engineering.
- Examine methods for verifying trust in a public key.
- Examine reasons that Internet users seek anonymity.
- Examine the concept of Privacy by Design (PbD) and enumerate its seven foundational principles.
- Examine the limitations of TOR.
- Examine the privacy responsibilities in different parts of an organization.
- Explain how encryption is used on mobile phones.
- Explain how to verify software downloads.

- Explain key fingerprints.
- Explain steps to use TOR safely and the reasons the steps are needed.
- Explain the concept of reputation risk.
- Explain the intended purpose of TOR
- Explain the relations between privacy frameworks and privacy engineering requirements.
- Explain the role of a key logger.
- Explain the role of network scanning in circumventing privacy.
- Explain the Web of Trust.
- Explain uses of creating ASCII-armored encryption.
- Explain why different key pairs are used for digital signatures and encryption.
- Explore the connections between privacy and data governance/data stewardship.
- Export a public key of a key pair.
- Generate a public key.
- Identify hidden services in TOR.
- Implement privacy best practices using a Privacy Impact Assessment during the QA process.
- Import a public key into GnuPG.
- Identify the role of the International Mobile Subscriber Identity (IMSI).
- Install and use GnuPG.
- Install and use Signal to end-to-end encrypt mobile communications.
- Install and use TOR.
- List methods by which identity can be determined on network devices.
- List some of the privacy frameworks established by governments and other entities.
- Locate keys from a public key server.
- Outline a privacy lifecycle engineering model.
- Outline an effect data governance program.
- Outline processes for authorizing the use of personal information and the forms of consent.
- Outline the benefits of digital signatures including authentication, integrity and non-repudiation.
- Outline the challenges of engineering a privacy system.
- Outline the key revocation process.
- Outline the needs for key expiration and revocation.
- Outline the privacy engineering development process.
- Outline the process of signing, compressing, and encrypting data.
- Outline the use of checklists in Quality Assurance.
- Review cultural aspects of privacy.
- Review four methods of location tracking for mobile devices.
- Review privacy concerns in an Agile environment.
- Review the effectiveness of turning off mobile phones to ensure privacy.
- Review the types and uses of mal-ware that may be found on mobile phones.
- Safely erase a file.
- Sign trusted keys locally.
- Speculate on the classification of meta-data.
- Step through the phases of a Privacy Impact Assessment.
- Trace the history of the modern concept of privacy.
- Trace the roles of participants in the Privacy Impact Assessment.
- Use GnuPG to edit keys.
- Verify different types of signatures.

OVERVIEW OF COURSE GRADING

The grades earned for the course will be derived using City University of Seattle's decimal grading system, based on the following:

Overview of Required Assignments	***% of Final Grade***
Virtual Labs	**45%**
• Lab 1: Performing Reconnaissance from the WAN	5%
• Lab 2: Scanning the Network on the LAN	5%
• Lab 3: Using Social Engineering Toolkit (SET)	5%
• Lab 4: Attacking the Firewall and Stealing Data Over an Encrypted Channel	5%
• Lab 5: Using Public Key Encryption to Secure Messages	5%
• Lab 6	10%
a. Provisioning a MySQL	3%
b. Database Provisioning PHP	3%
c. PHP Sessions and Cookies	4%
• Lab 7: Additional SCRIPT Elements	5%
• Lab 8: Remote Reflected XSS Mitigation and URL Encoding	5%
Papers	**35%**
• Paper 1: International Privacy Paper	20%
• Paper 2: Privacy Training Plan	15%
Instructor Assignments & Discussions	**20%**
• The Muddiest Point	5%
• Discussion	15%
TOTAL	**100%**

SPECIFICS OF COURSE ASSIGNMENTS

The instructor will provide grading rubrics that will provide more detail as to how this assignment will be graded.

Virtual Labs

The student will complete required number of virtual labs. The lab exercises involve the viewing of instructional videos and following step-by-step instructions to connect to virtual devices in a simulated environment to control, configure, manage and monitor those devices, as well as simulate security exploits. Activities are embedded within each lab, these activities present a challenge to complete and on completion of the challenge the student is rewarded with a milestone. Each lab will be graded on accuracy. The student has unlimited attempts at each lab to increase their accuracy and skill.

Grading Components *	% of Grade *	Below Standard	Approaching Standard	At Standard	Exceeds Standard
Accuracy of Solutions	100	0.00-68.74% of accuracy on lab.	68.75-86.24% accuracy on lab.	86.25 - 93.74% accuracy on lab.	93.75 - 100% accuracy on lab.
Total	100				

- Lab 1: Performing Reconnaissance from the WAN
- Lab 2: Scanning the Network on the LAN
- Lab 3: Using Social Engineering Toolkit (SET)
- Lab 4: Attacking the Firewall and Stealing Data Over an Encrypted Channel
- Lab 5: Using Public Key Encryption to Secure Messages
- Virtual Lab 6.a: Provisioning a MySQL
  Virtual Lab 6.b: Database Provisioning PHP
  Virtual Lab 6.c: PHP Sessions and Cookies
- Virtual Lab 7: Additional SCRIPT Elements
- Virtual Lab 8: Remote Reflected XSS Mitigation and URL Encoding

Papers

- Paper 1: International Privacy Paper
- Paper 2: Privacy Training Plan

Paper 1: International Privacy Paper

Students will compare and contrast privacy laws and regulations across two countries, other than the US, in different regions. The paper will include an analysis of the historic and cultural influences which shapes the laws. The paper should include how the laws and regulations would affect privacy policies for a company which operates in both jurisdictions as well as the US. This would include issues and conflicts that arise in shaping the policy. References to US laws and regulations may be used to guidepost the discussions.

Components	***% of Grade***
Privacy Policy Development	50%
Clear, concise, grammatical written communication	30%
References	20%
TOTAL	**100%**

Paper 2: Privacy Training Plan

Students will complete a privacy training plan and presentation which covers the Generally Accepted Privacy Principles (GAPP) or related topics and deals in particular with the identification and handling of personal or classified data.

As the first step, each student will determine an audience for the training and pattern the training toward that audience.

The deliverables include a lesson outline and visual presentation materials. The lesson outline should include an identification of the intended audience.

Students are encouraged to provide their presentation to the targeted audience even though it is not a requirement of the assignment.

Components	*% of Grade*
Private and Classified Info	20%
Privacy Policy Development	30%
Requirements	20%
Visual Presentation	30%
TOTAL	**100%**

Instructor Assignments & Discussions
Students will participate in activities and discussion as defined by the instructor. Whether in class, online, or in a mixed mode setting, students will be graded on their participation in classroom discussions; their ability to present, explain, or defend alternative viewpoints; and the degree to which they have mastered the concepts and principles inherent in the study of systems and application information/digital security. Written work will be assessed not only on relevance to the subject presented, but also on adherence to good written form and professional presentation. In this class, these activities build upon the common case study used in the virtual labs and knowledge and skills learned; thus, permitting students to socialize and debate the concepts and ideas. The instructor may also choose to create additional activities to support learning in the classroom or online. Online classes are required to use the Discussion Board. Participation through discussion is an integral part of this course and is defined as active engagement in a discussion or other activity. Instructors will determine the type of activities and their due dates; moreover, different activities will have different guidelines with regard to substance and length. The instructor will provide specific instructions to students.

The Muddiest Point
Each week, students are required to finish the muddiest point activity before starting their class.
The purpose of this activity is not to evaluate your knowledge but to encourage your engagement in class.
This activity consists of an essay question called the muddiest point and a couple of multiple choice questions.

The Muddiest Point is another general Classroom Assessment Technique (CAT), in which we can assess how well students are comprehending key points during a lesson or a course.
This technique asks students to briefly state what part of the assignment was most confusing for them.

This activity must be done before the next class.

Discussion Board
All classes are required to use the Discussion Board. Participation through discussion is an integral part of this course and is defined as active engagement in a discussion or other activity. Instructors will determine the type of activities and their due dates; moreover, different activities will have different guidelines with regard to substance and length. The instructor will provide specific instructions to students.

A discussion question or topic from the instructor appears weekly in the Discussion Board. Students are to post their answers as well as responses to two other students' responses in the Discussion Forum by the end of each session. The forum is to help promote student to student discussion. The instructor may not respond to each posting. Questions or comments that are specifically for the instructor, should be emailed directly to the instructor or posted in the Question and Answer Forum. Students who want to talk with other students about issues unrelated to the discussion forums should use the Coffee Talk Forum.

Although the tone of your discussion board postings can be informal, your instructor will expect the content to be on a professional level. In other words, your comments and questions for discussion should

be clear and thoughtful, with correct grammar, spelling, and punctuation. As with written assignments, the quality of your discussion postings will be graded on both content and presentation.

Components	***% of Grade***
Quality Discussion Participation	60%
Meets requirements in a timely manner	20%
Writes clearly, concisely, and grammatically	20%
TOTAL	**100%**

COURSE POLICIES

Late Assignments

LATE ASSIGNMENT

Participation

PARTICIPATION

Professional Writing

Assignments require error-free writing that uses Standard English conventions and logical flow of organization to address topics clearly, completely, and concisely. CityU requires the use of APA style.

UNIVERSITY POLICIES

You are responsible for understanding and adhering to all of City University of Seattle's academic policies. The most current versions of these policies can be found in the University Catalog that is linked from the CityU Web site.

Scholastic Honesty

Scholastic honesty in students requires the pursuit of scholarly activity that is free from fraud, deception and unauthorized collaboration with other individuals. You are responsible for understanding CityU's policy on scholastic honesty and adhering to its standards in meeting all course requirements. A complete copy of this policy can be found in the University Catalog in the section titled *Scholastic Honesty* under *Student Rights & Responsibilities*.

Attendance

Students taking courses in any format at the University are expected to be diligent in their studies and to attend class regularly.

Regular class attendance is important in achieving learning outcomes in the course and may be a valid consideration in determining the final grade. For classes where a physical presence is required, a student has attended if s/he is present at any time during the class session. For online classes, a student has attended if s/he has posted or submitted an assignment. A complete copy of this policy can be found in the University Catalog in the section titled *Attendance Policy for Mixed Mode, Online and Correspondence Courses*.

SUPPORT SERVICES

Disability Resources

If you are a student with a disability and you require an accommodation, please contact the Disability Resource Office as soon as possible. For additional information, please see the section in the University Catalog titled *Students with Special Needs* under *Student Rights & Responsibilities*.

Library Services

CityU librarians are available to help you find the resources and information you need to succeed in this course. Contact a CityU librarian through the *Ask a Librarian* service, or access library resources and services online, 24 hours a day, seven days a week.

Smarthinking

As a CityU student, you have access to 10 free hours of online tutoring offered through Smarthinking, including writing support, from certified tutors 24 hours a day, seven days a week. Contact CityU's Student Support Center at help@cityu.edu to request your user name and password.