Repository Entry for CS 145
Embedded EthiCS @ Harvard Teaching Lab
Cat Wade

NOTE: this module should be labeled as "under development."

Overview	
Course: CS 145/245: Cloud Networking and Computing	
Course Level: Upper-level undergraduate and graduate	
Course Description: "Clouds have become critical infrastructures for many applications in business and society (e.g., social media, public health, and entertainment). In this course, we will take a look inside the cloud infrastructure and learn critical technology trends and challenges in the networking and computing layers. We will discuss the design choices of performance, scalability, manageability, and cost in various cloud companies such as Amazon, Google, Microsoft, and Facebook. This course includes lectures and system programming projects."[1]	
Module Topic: The Ethics of Cloud Security	
Module Author: Cat Wade	
Semesters Taught: Spring 2019	
Tags: rights [phil], moral responsibility [phil], privacy [phil], stakeholders [phil], cloud networking [cs], cloud security [cs], cloud computing [cs], ddos attacks [cs], value [phil]	
Module Overview: In this module, we discuss why computer security matters from an ethical perspective, focusing on the special case of cloud security (security for cloud computing systems). More specifically, the module focuses on three issues. First, we consider the varying reasons different groups of stakeholders, such as service providers and end users, have to care about cloud security. Second (and relatedly), we discuss the connection between cloud security and privacy. Third, we consider who is morally responsible for maintaining cloud security and how to determine responsibility when it is breached.	
Connection to Course Technical Material: This course focuses on the technical aspects of data storage and management in the cloud context. The module comes right at the end of the "cloud management" portion of the semester and builds directly on technical material the students have just covered by considering ethical questions raised by real world examples of cloud security breaches.	

[1] http://minlanyu.seas.harvard.edu/teach/cs145-spring19/index.html

Goals	
Module Goals: ● Identify general reasons for valuing computer security from an ethical perspective. ● Consider how those general reasons to value security apply to real-world case studies featuring cloud computing systems. ● Practice communicating about the ethical importance of cloud security in different contexts. ● Practice communicating about the ethical importance of cloud security in a range of different contexts, for example, to colleagues, to peers, to potential customers ● Identify conflicts between different reasons to value security and consider how to resolve those conflicts. ● Analyze relevant features for responsibility and communicate about their role in case studies. ● Identify and analyze those features of cloud security cases that are relevant for assessments and ascriptions of moral responsibility and practice communicating about responsibility accurately using these features	
Key Philosophical Questions: 1. Why do we value computer security? 2. Do different groups of stakeholders have different reasons to value computer security? 3. How do we make sense of holding groups (e.g. entire corporations) responsible? 4. How should we trade off computer security and privacy when the two come into conflict? 5. What determines who is morally responsible for a cloud security breach?	
Materials	
Key Philosophical Concepts: ● Value ● Privacy ● Moral responsibility	
Assigned Readings: The students were assigned the following two optional readings: ● Ristenpart, et. al. (2009), “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds.” https://hovav.net/ucsd/dist/cloudsec.pdf.	

• Marczak et. al. (2015), "An Analysis of China's "Great Cannon." https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf.	
Implementation	
1. What is cloud security? 2. Cloud security case studies. 3. Reasons to value security. 4. Addressing conflicts between security and privacy. 5. Who is responsible for cloud security breaches? 6. Concluding discussion.	
Sample Class Activity: In this activity, students break up into small groups and consider three real-world cases in which the security of a cloud computing system was compromised: 1. *GitHub DDOS attack.* February 2018: Code repository website GitHub is subjected to a 'Distributed Denial of Service' (DDOS) attack, wherein their servers were intentionally flooded to beyond capacity in order to render their service unusable for a period of time 2. *Facebook storing passwords in plaintext on internal servers.* March 2019: Facebook announces that tens of thousands of passwords for Facebook-owned platforms, including Instagram, are stored in plaintext (i.e., unencrypted) on internal servers and therefore were accessible to Facebook employees 3. *Celebrity iCloud photos hack.* August 2014: A number of celebrities are targeted via 'phishing' attacks, attacks where hackers pose as legitimate companies asking for passwords and other sensitive information to be shared. Access to iCloud photos is then made possible, and a number of sensitive photos are 'leaked' across the internet. Students are asked to answer two questions about each case: 1. What groups of stakeholders were affected by the security breach in question, and what reasons do they have to be concerned about the breach? 2. Who should be held responsible for the breach and why? After the small-group discussion, the Embedded EthiCS fellow leads a debrief with the full class.	
Module Assignment: In this assignment, students are asked to write a short essay discussing the value of cloud security in the following hypothetical case study:	

GDPR TEETHING PAINS: It is May of 2018. You are the manager of a small European company that uses cloud services to manage and store personal customer information. Consequently, with GDPR on the horizon, you have to begin to prepare your employees and customers for the changes and disruptions that will come about as a result of meeting these new regulations. In the essay, students first identify and explain one of the reasons to value cloud security discussed in class. Second, they appeal to this reason in order to justify the costs involved in satisfying the new GDPR regulations to two different groups of stakeholders: their customers, and their employees.	
Lessons Learned: ● Students are especially engaged in a technical CS course like this by philosophical discussion that attends to more concrete technical problems. Future iterations of this module would be benefitted by balancing the sometimes very abstract concepts with more extensive discussion of technical examples.	