CS 263. Repository Entry
Embedded EthiCS @ Harvard Teaching Lab

Overview

Course:	CS 263 Systems Security	
Course Level:	Upper-level undergraduate	
Course Description:	"This course explores practical attacks on modern computer systems, explaining how those attacks can be mitigated using careful system design and the judicious application of cryptography. The course discusses topics like buffer overflows, web security, information flow control, and anonymous communication mechanisms like Tor. The course includes several small projects which give students hands-on experience with various offensive and defensive techniques; the final, larger project is open-ended and driven by student interests"[1]	
Module Topic:	The Ethics of Hacking Back	
Module Author:	Elís Miller Larsen	
Semesters Taught:	Fall 2020	
Tags:	Systems [CS] Systems security [CS] hacking back [CS] active cyber defense [CS] moral permission [phil] moral obligation [phil] decision-making [phil] justification [phil] reasons [phil]	
Module Overview:	This module focuses on a practical question for engineers working on systems security: Is hacking back ethical? Students are asked to consider how they would respond in situations that might require hacking back and come up with reasons that might make hacking back permissible or impermissible. Overall, students should leave the module with a clear sense of the problem of hacking back, the risks that are attributed to hacking back, and why the answer to the problem is not a simple solution of "getting your stuff back." They should be able to generate reasons in favor and against a decision to hack back that is logically tractable and morally justifiable.	Marginal notes
Connection to Course Material:	Students spend the first part of the course learning how to mitigate threats by shoring up vulnerabilities of systems. This module connects to these techniques of system defense by introducing the next step of defense: responding to a security breach. A discussion of the ethics of hacking back places the students in a situation where their system defenses have failed, and they need to determine the next step to protect proprietary information.	This topic works well because of its direct connection to the technical materials of the course. It is also a timely topic, in the sense that students will be familiar with the idea of systems being hacked, or the potential need for hacking back (e.g. recent political hacking via social media). Another topic that would be apt for this course is "hacktivism". Hacking back introduces the idea of cyber vigilantes, and it became clear through the discussion that students were interested in the

[1] Insert hyperlink to source (e.g. Harvard course catalogue)

		moral considerations of cyber vigilante work.

Goals		
Module Goals:	1. Identify why hacking back [CS] is an ethical issue. 2. Introduce moral permission [phil] and moral obligation [phil] as philosophical tools to analyze the problem of hacking back. 3. Introduce reasons [phil] as a way to determine whether decisions are justified [phil] in examples of hacking back. 4. Address how reasons are value laden so that ethical decisions are impacted by different considerations, perspectives, and power dynamics.	Marginal notes
Key Philosophical Questions:	1. What are some of the most significant reasons that count for and against hacking back? 2. When is a decision to hack back morally permissible? 3. When is a decision to hack back morally required?	The reasons these questions were chosen is to highlight the ethical and practical decisions that students might face as engineers. Question 1 focuses on an analysis of whether hacking backing is something individuals and corporations are morally allowed to do. And Question 2 focuses on an analysis of whether there are some cases when hacking back would be required. These cases would be similar to other ethical cases where seeing evil and doing nothing would be impermissible. Question 2 also connects nicely with the second assigned reading from the New Yorker that is an introductory assessment of cyber vigilantism.

Materials		
Key Philosophical Concepts:	● Moral permission ● Moral obligation/requirement ● Decision-making ● (Moral) Reasons	The concepts of moral permission and moral obligation are used in order to explore the key philosophical questions of the module. Both concepts can be explicated in part by the idea of justification, which we cash out for the purposes of this module in terms of reasons.
Assigned Readings:	● "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies," Patrick Lin ● "The Digital Vigilantes Who Hack Back," Nicholas Schmidle	The first reading is a philosophical publication that provides six arguments: half that support hacking back and half that do not

		support hacking back. These arguments touch on philosophical issues, such as social contracts, property and self-defense. The philosophical analysis of these issues in the paper is limited, however, so if one wants to utilize the philosophical ideas of the paper, additional readings would need to be assigned. The second reading is a journal article from the *New Yorker* that examines the ethics of hacking back, by proposing that hacking back is vigilante work. This article is exceptional and is helpful for getting students to recognize how the legal domain is not currently a reliable resource for dealing with the issue of hacking back.

Implementation

Class Agenda:	1. Overview of the ethical problem at hand: why hacking back is an ethical issue. 2. Introduction of key philosophical concepts and frameworks: Moral permission, moral obligation, and reasons. 3. Activity: The Hackback Dilemma 4. Questions/Discussion	Marginal notes
Sample Class Activity:	Using Google Forms for response entries, students were provided a scenario that placed them as the decision maker for hacking back. In the scenario, the student is a senior systems security engineer for Google. They learn that information for a new application has been stolen, and this application has already been enthusiastically approved by shareholders and higher-ups at Google. Students are asked to decide whether or not they would hack back to retrieve the information and whether they thought their decision was morally permitted or morally required.	There are two ways this activity can be updated. 1. Use different scenarios. The Google case is a hypothetical scenario developed by the TA and the course head. It might be more useful to use a real-life scenario to connect the activity to other content learned in the course. For example, one could use the Zeus malware scenario as a real-life case that is often discussed as part of the ethics of hacking back. 2. Apply a game-theoretic approach to the google form (see "Lessons Learned") and play a version of the Prisoner's

		Dilemma. Instead of having students respond to the form, Google forms can be used for students to "play" against each other. The activity would require that in the scenario one student acted as the hacker and the other student the systems security engineer. Both students would need to make choices about when they should hack and when they should not hack. The activity would bring out how hacking back may be a kind of "tragedy of the commons" because individuals and corporations need to find ways to engage and cooperate in the cyber domain. These decisions rest with individual players because there are no official laws about hacking back.
Module Assignment:	Students were asked to give a brief, two-sentence response to the reading. One sentence to outline something they found interesting, and another sentence to say what they found confusing, or ask a question.	
Lessons Learned:	From the discussion it was clear that students needed some direction when it came to understanding how attribution played a major role in the decisions we would want to think about with respect to hacking back. Especially, the idea that if one hacks back, it could be traced back to you. Once students understood that the hack back could be traced back, responses to the ethics of hacking back changed. There was also a lot of interest in hacktivism, and the ethical implications of vigilante work. It may be worthwhile to have an entire module just on "Hacktivism". This module would work well with the second activity update listed above. Students used Edward Snowden as an example where it might be ethical to hack in the first place, which changes whether hacking back would be ethical. This idea works well with a game-theoretic approach to the activity where students play a version of Prisoner's Dilemma. This game	

	would help students recognize that their decisions are not isolated and impact others and encourage them to consider scenarios in which it is not clear that the hacker is a “bad guy.” Hacking back might turn out to be impermissible in cases in which the initial hacking itself was permissible, perhaps even obligatory.	