Overview

Course:	CS 263: Systems Security
Course Level:	Graduate
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 such as 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:	Sophie Gibert
Semesters Taught:	Fall 2021
Tags:	Hacking [CS], systems [CS], systems security [CS], active cyber defense [CS], attribution [CS], justification [phil], moral rights [phil], rights [phil], rights infringement [phil], rights violation [phil], self-defense [phil], proportionality [phil], deterrence [phil], retribution [phil], rights-forfeiture [phil], standing to punish [phil], social value [phil]
Module Overview:	This module focuses on a practical question for engineers working in systems security and cyber defense: Is hacking back ever morally justified? The module begins with an explanation of why hacking back is an ethical issue, emphasizing that hacking back can cause great harm and that it usually disrespects important moral rights. It then guides students through a four-step case analysis, which illuminates some potential justifications for hacking back.
Connection to Course Material:	Students in this course learn how to mitigate and respond to cyberattacks using both offensive and defensive techniques. This module poses questions about when, if ever, it is morally justified to employ offensive techniques.
	The topic was chosen because of its direct connection to the technical material covered in the course. The topic is also timely: several instances of hacking back have been covered in recent media, and legislation has recently been proposed in the US that would legalize hacking back - namely, the Active Cyber Defense Certainty Act (or "Hack Back" bill).

Goals

Module Goals: By the end of the module, students should be able to:

1. Define hacking back and describe its various purposes.
2. Explain why hacking back requires moral justification by appealing to the notions of harm and moral rights.

[1] Link.

	3. Explain why most instances of hacking back are not self-defensive and why this fact matters, ethically speaking. 4. Identify several potential justifications for hacking back. 5. Make a preliminary judgment about whether hacking back is morally justified in a realistic, hypothetical scenario.	
Key Philosophical Questions:	1. What is hacking back? 2. Why does hacking back require moral justification? 3. Why are most instances of hacking back not instances of self-defense, and why does this fact matter, ethically speaking? 4. What are some potential justifications of hacking back, and under what circumstances might they apply?	Questions 1 and 3: The term "hacking back" is used in a variety of different ways in the media and scholarly literature. It is often used interchangeably with the term "active cyber defense," which leads many to assume that hacking back is a form of self-defense, which it usually is not. Question 2: It is likely that students are familiar with the potential harms of hacking back but not with the idea that hacking back usually disrespects moral rights.

Materials		
Key Philosophical Concepts:	● Moral justification ● Moral rights ● Rights infringement and violation ● Self-defense ● Proportionality and necessity ● Deterrence ● Retribution ● Rights forfeiture ● Standing to punish ● Social value	Section 1 of the module explains: that hacking back risks causing harm to others and usually disrespects important *moral rights*; that such acts require *moral justification*; that when one justifiably disrespects a right, one merely *infringes* it, while when one unjustifiably disrespects a right, one *violates* it; and that hacking back usually isn't self-defensive, but that when it is, it does not disrespect rights, as long as it is necessary and proportionate. Section 2 of the module leads students through a case analysis that illuminates potential justifications for hacking back, including that hacking back may *deter* hackers, that hacking back may generate *social value* in certain circumstances, and that hacking back may serve as a form of *retributive justice*, provided that

		wrongdoers *forfeit rights* against proportionate punishment and that victims of hacking have *standing to punish*.
Assigned Readings:	● Schmidle, Nicholas. "The Digital Vigilantes Who Hack Back." ● Lin, Patrick. "Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies."	Schmidle tells the story of a hack-back that many consider to be morally justified. His article brings the topic of hacking back to life and highlights its timeliness. Lin discusses six common arguments for and against hacking back. It provides a balanced overview of the topic and serves as a good example of analytical writing.

Implementation

Class Agenda:	1. Explanation of what hacking back is and why it is an ethical issue (that it risks causing great harm, that it usually disrespects important moral rights). 2. Explanation of why hacking back typically isn't self-defensive and why this fact matters. 3. Class activity/discussion. 4. Explanations of retribution and rights-forfeiture, deterrence, and social value.	
Sample Class Activity:	Students are given a hypothetical scenario involving hacking back, designed by the teaching team in conjunction with the course's professor. They are led through a case analysis, guided by four questions: 1. Would hacking back disrespect any important moral rights? Hint: Consider whether hacking back would be self-defensive in this case. 2. What are the likely harms of hacking back? 3. What are the likely benefits of hacking back? 4. Is hacking back morally justified? Students discuss each question in pairs and share their responses with the class; key takeaways are solidified before moving on to the subsequent question.	Discussion in pairs, rather than small groups, is appropriate for this class because it takes place in a tiered lecture hall.
Module Assignment:	Before class, students are asked to give a brief, two-sentence response to the reading that identifies something they found interesting, identifies something they found confusing, and asks a question.	The professor designs and grades the post-class assignment.

	After class, students engage with ethics on a portion of the problem set. At the end of their problem set on reverse-engineering, they are told to imagine that, as part of a job at a software company called WidgetCo, they have been asked to reverse-engineer a server belonging to a cyberattacker who stole property from WidgetCo. The goal of reverse-engineering the server would be to discover a vulnerability that can be exploited in a counter-attack. WidgetCo, students are told, thinks that performing a hack-back would be justified in this case because the cyberattackers are known to be planning another attack on WidgetCo, as well as another company. Students are asked: “How would you respond to the request from WidgetCo to actively destroy the attackers' server? Which arguments from "Ethics of Hacking Back" by Patrick Lin would influence your decision?”
Lessons Learned:	Student responses to this module were overwhelmingly positive. Students appreciated the discussion of whether hacking back ever constitutes self-defense and found the distinction between infringing and violating moral rights to be particularly helpful. Pedagogical lessons learned: ● The four-step case analysis activity works well pedagogically, but care should be taken to ensure that there is enough time to get through all four steps. ● Infusing modules with real-world examples and technical applications goes a long way in ensuring student engagement. ● Students appreciate having philosophical concepts and distinctions to structure their analysis of ethical problems.