A Case Study in Malware Research Ethics Education

When teaching bad is good

John P Sullins
Department of Philosophy
Sonoma State University
1801 East Cotati Ave.
Rohnert Park, CA 94928
Email: john.sullins@sonoma.edu

Cyber-security Research
Ethics Dialog & Strategy
Workshop (CREDS II -
The Sequel)
San José, May 17, 2014

SONOMA
STATE UNIVERSITY

Introduction

- Academic malware research is on the rise
- Professor George Ledin, SSU
- John Aycock, Calgary

presentation outline
- topics in ethics presented in the class
- How they are presented and assessed
- rationale for requiring students to keep ethical norms in mind as they do their research projects involving malware design

The team behind the SSU malware research course.
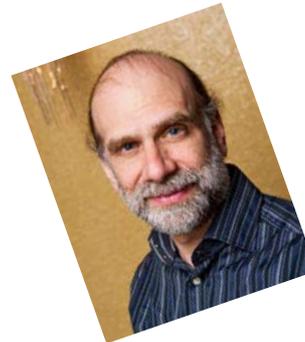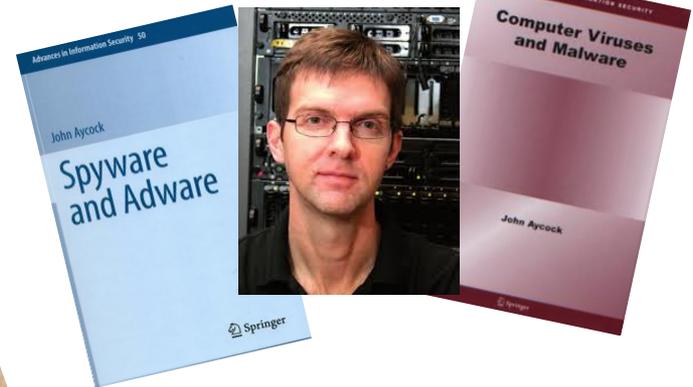The Author, George Ledin, and Roger Mamer.
http://www.sonoma.edu/insights/archive/08fall/malware_class.shtml

MALWARE ETHICS

Background and Research Collaboration

- Malware Ethics has been slow to emerge
  - Oxymoron for ethicists
- On the other hand…
  - George Ledin
    - Must know the enemy to defeat them
  - John Aycock
    - Malware can be ethically and artistically designed
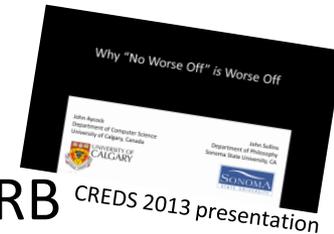 - And others
    - Teaching malware is a public good

Teaching this stuff is just plain smart.
Bruce Schneier, June 12, 2007
https://www.schneier.com/blog/archives/2007/06/teaching_viruse.html

Ethical Problems in the Study of Malware

- Human Subjects
  - "No worse off"
  - Problems with IRB

- Malware and Information Ethics
  - Recording data and informed consent
  - Communicating dangerous findings
  - Synthesizing or acting on data in unethical ways

Why "No Worse Off" *is* Worse Off

John Aycock
Department of Computer Science
University of Calgary, Canada

John Sullins
Department of Philosophy
Sonoma State University, CA

CREDS 2013 presentation

CASE STUDY—A COURSE IN MALWARE ETHICS

Rationale

- Traditional computer ethics
  - Some help here
- Medical ethics
  - Some help also but mostly it is too specific to medicine
- We must rethink ethics for the milieu of malware

SSU computer science student Ben Corr demonstrates for fellow students his project, which attempts to bypass security and gain access to a computer set up in class. (MARK ARONOFF / PD)
http://www.pressdemocrat.com/article/20070522/news/705220312

Basic Ethics Concepts Taught

- Start with ACM Code of Ethics
  - But malware research quickly contradicts these rules
- Greatest hits in ethics
  - Utilitarianism
  - Deontology
  - Human rights
  - Unified common goods approach of James Moor
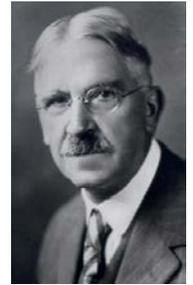 - Virtue ethics
  - Information ethics

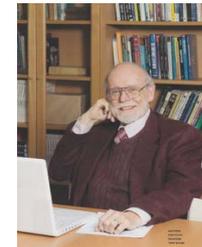- Some of my influences (In no particular order of importance)

All of this with an eye towards: privacy, digital property rights, digital divide, gender and identity politics, etc.

Deborah Johnson

James Moor

John Dewey

Mario Bunge

Luciano Floridi

Terrell Ward Bynum

Charles Ess

And many more…

Virtues in Security

- Virtue is culturally dependent
  - What are virtues in the security community?
    - Professional virtues
    - Software virtues
      - CIA
        - Confidentiality
        - Integrity
        - Availability

- We critique
  - Firewall illusion
  - Data level security
  - Personal encryption
  - Cyberwarfare ethics

- Some of my influences in this area

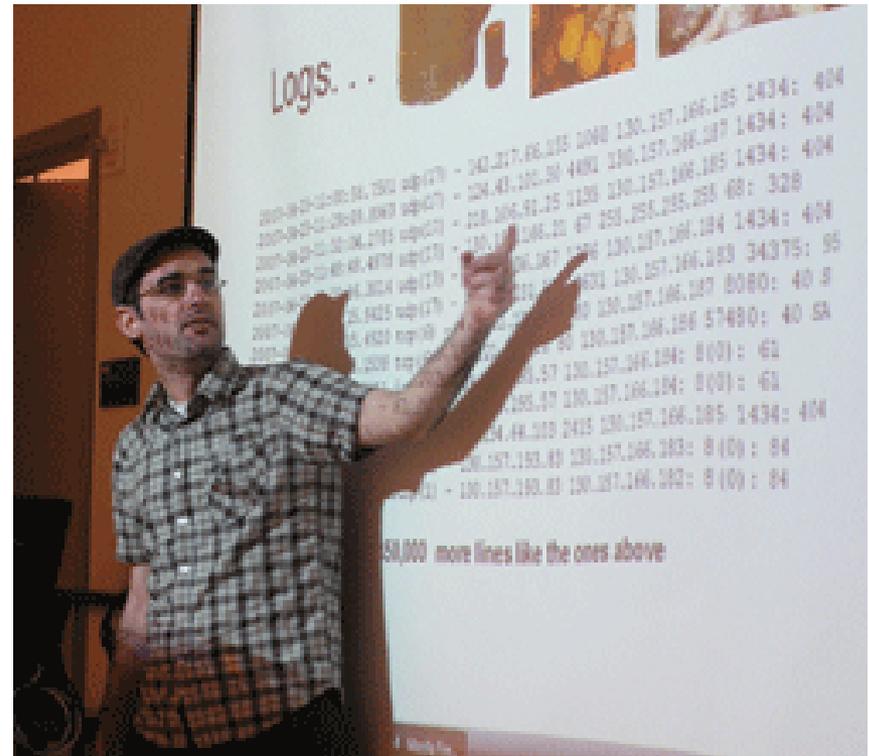Shannon Vallor

Mariarosaria Taddeo

Ethical Hacks

Student Lincoln Peters sits at the helm of a closed network of four operating systems which are used to test malware he has designed. Photo by Roger Mamer.
http://www.sonoma.edu/insights/archive/08fall/malware_class.shtml

- Students are not treated as passive receptors of ethical thought
  - Active agents creating new ethical norms
  - Building ethical commitments to each other and society
  - Therefore we focus on personal motivations
  - Personal codes of conduct are more important and decisive than any institutionally produced code of ethics
- Assessments
  - Discussion and reflection
  - Quizzes
  - Ethical warrants analysis on projects
  - Personal ethos statement

Conclusions

- Must not overlook ethics in malware research
- Teach ethics early on
- Focus on special challenges of malware research
- Keep it personal
- We are an example of a successful implementation of these ideas

Student Mike Drew demonstrates the workings of a "Honeypot," a system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computers.
http://www.sonoma.edu/insights/archive/08fall/malware_class.shtml