The Need for Community Standards for Ethical Behavior in Computer Security Research

Michael Bailey

University of Michigan

IFIP WG 10.4

January 16th, 2011

Snowmass, CO

Do the Right Thing

Building An Active Computer Security Ethics Community, by David Dittrich, Michael Bailey, and Sven Dietrich, IEEE Security and Privacy (pre-publication), December 16, 2010.

- Researchers want to help, to benefit the *internet community*
- …but oh, the temptations!

  First to publish; do something new; show how 31337 you are; fight for funding; ends justify the means
- …and the conflicts

  Affecting other research; impacting LE investigations; thwarting mitigation efforts; protecting rights; helping the bad guys; less risky (and less sexy) options?

This is where Ethics come in…

What are ethics?

- “The field of ethics (or moral philosophy) involves systematizing, defending, and recommending concepts of right and wrong behavior.”
- Normative ethics, is concerned with developing a set of morals or guiding principles intended to influence the conduct of individuals and groups within a population (i.e., a profession, a religion, or society at large).
  - Consequentialism
  - Deontology
  - virtue ethics

Computer Ethics

"A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with **new capabilities** and these in turn give us **new choices** for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine **what we should do** in such cases, i.e., to formulate policies to guide our actions."

-Moor

Existing Ethics Standards

- The IEEE, ACM, etc: **Codes of Ethics**
- **The Belmont Report**, the National Research Act, and Institutional Review Boards (IRB)
    - 45 CFR 46
- **“Rules of Engagement”**
    - The **Law of Armed Conflict**
    - Dittrich/Himma: **Active Response Continuum**
- **Other Organizational Codes (Universities, Corporations, etc.)**

IRB and the Belmont report

- The primary goal of the Institutional Review Board (IRB) is to assure that, in research involving human subjects, the rights and welfare of the subjects are adequately protected.
- "Ethical Principles and Guidelines for the Protection of Human Subjects of Research", United States Department of Health, Education, and Welfare, April 18, 1979 (Belmont Report)
- Respect for persons
  - Individuals should be treated autonomously
  - Informed consent should be freely given
- Beneficence
  - Do no harm
  - Maximize possible benefits/minimize risks
- Distributive Justice
  - Equitable selection of research subjects

Professional Ethical Codes

- IEEE Code of Ethics (2006)
  - commits members ”to the highest ethical and professional conduct”. Members agree to avoid conflicts of interest, be honest, engage in responsible decision making, accept criticism of work, etc
- ACM Code of Ethics and Professional conduct (1992)
  - “contribute to society and human well-being”, “avoid harm to others”, along with six other principles (e.g., don’t discriminate, be honest, respect privacy).

Limitations of Existing Standards

- Lack of shared community values
  - Persistent chatter about papers, numerous years after publication
- Lack of individual expertise in formal ethical decision making
  - Who serves on an IRB?
  - Inconsistent application of principles
- Lack of agreement on enforcement
  - IRB?
  - PC?
  - ACM, IEEE, ISOC?
  - NSF, DHS, DARPA?

Limitations of Existing Standards

- Lack of shared community values
  - Persistent chatter about papers, numerous years after publication
- Lack of individual expertise in formal ethical decision m
- La
  - IRB?
  - PC?
  - ACM, IEEE, ISOC?
  - NSF, DHS, DARPA?

If we don’t get our act together, someone will do it for us.

Moving Forward

- Building personal decision making capabilities
- Consistency
- Integrity and Accountability
- Involvement
- Self Governance
- Take forward Lessons
- Reward Ethical Behavior

Building personal decision making capabilities: Stakeholder Analysis

David Dittrich, Michael Bailey, Sven Dietrich. Towards Community Standards for Ethical Behavior in Computer Security Research. Stevens CS Technical Report 2009-1, 20 April 2009

David Dittrich, Michael Bailey, and Sven Dietrich. Have we Crossed the Line? The Growing Ethical Debate in Modern Computer Security Research. In (Poster at) Proceedings of the 16th ACM Conference on Computer and Communication Security (CCS '09), Chicago, Illinois USA, November 2009

- **Primary** Stakeholders

  "Those ultimately affected [either positively or negatively]"

- **Secondary** Stakeholders

  "Intermediaries in delivery [of the benefits or harms]"

- **Key** Stakeholders

  "Those who can significantly influence, or are important to the success [or failure] of the project"

Stormfucker: Owning the Storm Botnet

- Presented at 25C3, Berlin, December 2008
  - University of Bonn students and faculty reversed Storm encryption and C&C protocol
  - Video at: http://mirror.informatik.uni-mannheim.de/pub/ccc/streamdump/saal3/
- Concerns
  - Risk/benefit (besides legality) not fully explored
  - Hadn’t fully reverse engineered Storm, or tested their tools on all Windows variants (but demo does work!)
  - Not running an enumerator, so didn’t know full population size/ constituency
  - Demonstrated that it worked, then released partial code to full-disclosure list

Stakeholders

Entity	Activity	Type	Risk/Benefit
Researchers	Discovered vulnerabilities thru RE, developed working exploit	Key	Reputation, altruism
Malware authors	Write and maintain malware, send spam, steal information, sell CaaS, observe Researchers	Key	Booty, Arrest
Svc. Providers	Support infected end users, receive spam, respond to abuse reports	Secondary	Lost revenue, DoS
End users (including enterprises)	Infected with bots, networks penetrated	Primary	Fraud, data loss, business continuity
General public	Receive services provided by enterprises (e.g., 9-1-1, health care, public services, banking, ecommerce)	Primary	Fraud, DoS, physical harm

Consistency: Ethical Impact Assessment (EIA) Framework

Erin Kenneally, Michael Bailey, and Douglas Maughan. A Tool for Understanding and Applying Ethical Principles in Network and Security Research. In Workshop on Ethics in Computer Security Research (WECSR '10), Tenerife, Canary Islands, Spain, January 2010.

- What:
  - A tool for assessing the privacy impact of a piece of work
- Why:
  - ‘unfunded mandates’ are a disservice to all stakeholders
  - make ethics ‘embraceable’ lower costs and increase motivation for researchers (especially technical mindsets) to engage
  - consistency

E.g. Applying Beneficence Principle

- Applied:
  - Do no harm
  - Minimize possible harms (& max benefits)
- Applied in cyber security context:
  - researchers should systematically assess both risks and benefits of research on privacy, civil rights, well-being of persons
    - Yeah, But RBA challenging with gaps, grayness of laws, professional codes, IRBs
  - researchers should consider the full spectrum of risks of harms to persons and information systems (reputational, emotional, financial, physical)
    - Yeah, But normative social immaturity re: harms (qualitative & quantitative)

EIA and Beneficence

- Example Framing Questions:
  - What are effects of research on all stakeholders: researchers, human subj, society?
  - What are possible unintended consequences? E.g., privacy harms
  - What is nature and source of collected data? What is purpose of collecting data? What is intended use of data?
  - Does research design include controls to minimize harms (ie, using in vitro, anonymization or other disclosure controls)?
  - What checks and balances to prevent/repeat harms?
    - break law
    - chill 1st A. rights to speak, associate, surf anonymously
    - target groups based on sex, religion, politics
    - cause harm – physical, financial, legal, reputational, psychological
    - Impair data quality & integrity
    - Surveillance harms – id theft, gov't persecution, alter behavior re: counter-surveillance
  - Could the research make the targeted problem (eg, infosec) worse, or undermine research goals?

Self Governance: Menlo Report

- DHS Working Group on Ethics in ICTR
  - Inaugural workshop May 26th-27th, 2009 in Washington, DC
  - Lawyers, Computer Scientists, IRB Members, Ethicists
- Goal is to create an updated Belmont report for the field of ICTR
- Initial feedback on draft report out for comments next month
- Public forum for discussion at IEEE Security and Privacy (Oakland): “*Community Workshop on Ethical Guidelines for Security Research*”

The Need for Community Standards for Ethical Behavior in Computer Security Research

Michael Bailey
University of Michigan

Questions? Comments?

mibailey@eecs.umich.edu
http://www.eecs.umich.edu/~mibailey