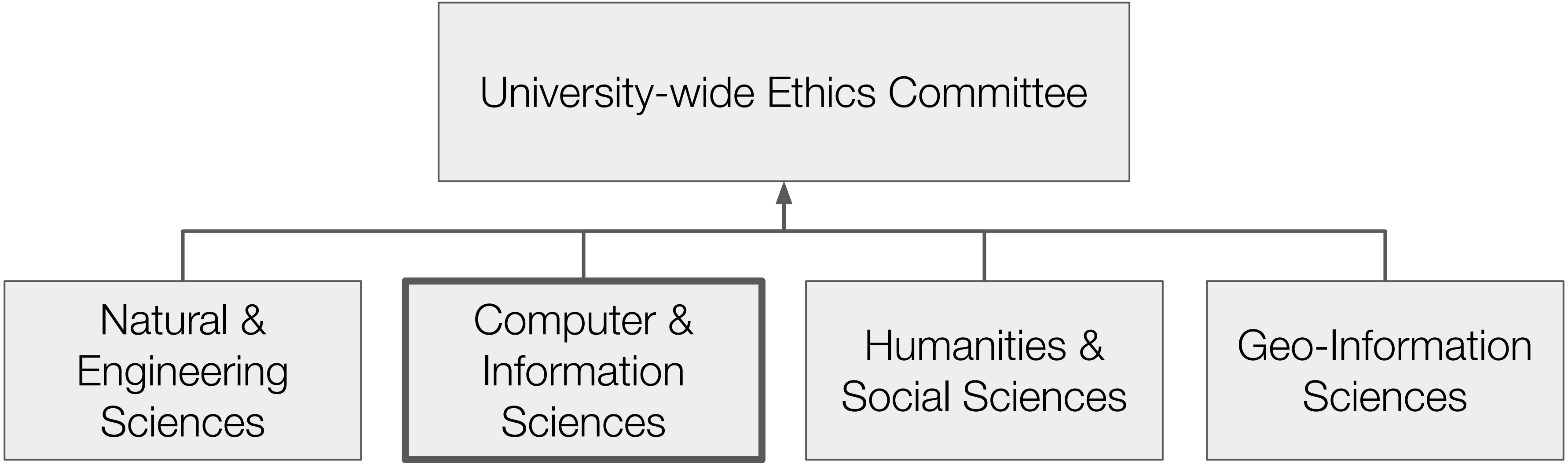
Operationalizing Cybersecurity Research Ethics Review: From Principles and Guidelines to Practice

Dennis Reidsma, Jeroen van der Ham, **Andrea Continella**

27 Feb 2023

UNIVERSITY
OF TWENTE.

Who we are



University-wide Ethics Committee

Natural & Engineering Sciences

Computer & Information Sciences

Humanities & Social Sciences

Geo-Information Sciences

What we do

Computer & Information Sciences Ethics Committee

- Human Computer Interaction design and user studies
- Internet-wide measurements
- AI, algorithms, and data science
- Cybersecurity
- (Limited) Medical applications

Why CS & cybersecurity ethics?

Prudent Practices for Designing Malware Experiments: Status Quo and Outlook

Ethical Considerations for Vulnerability Disclosure

Where research identifies a vulnerability (e.g., software vulnerabilities in a given program, design weaknesses in a

of vulnerability in deployed systems), we expect that researchers act in a way that avoids gratuitous harm to affecte

disclosing the vulnerability to vendors of affected systems, a

On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits

IT'S NOT HUMAN SUBJECT RESEARCH
HUMANS ARE EVENTUALLY AFFECTED BY THE RESEARCH
imgflip.com

How to make cybersecurity research ethics review practical?

Disclaimer: We do not want to define a set of strict rules, as guidelines should be adapted to better fit local law, regulations, etc.. This “works for us”

Three-step approach

1. Review and identify risks, together with their related principles
2. Define a strategy for a self-assessment questionnaire
3. Formalize questions and assess their effectiveness

...and repeat...

Ethics risks in CybSec research

R1 Accidental discovery *(Privacy, Consent)*

R2 Publication of private data *(Privacy, Consent)*

R3 Damaging production systems *(No Harm)*

R4 Misuse by malicious actors *(Misuse; Dual Use/Military Applications)*

R5 Discovering vulnerabilities *(No Harm)*

R6 Reprisal against researcher *(Researchers' well-being)*

R7 Lack of consent *(Consent)*

R8 Damaging people or companies *(No Harm, Consent)*

R9 Illegal behavior by researcher *(Consent, Deception, Illegality, Well-being)*

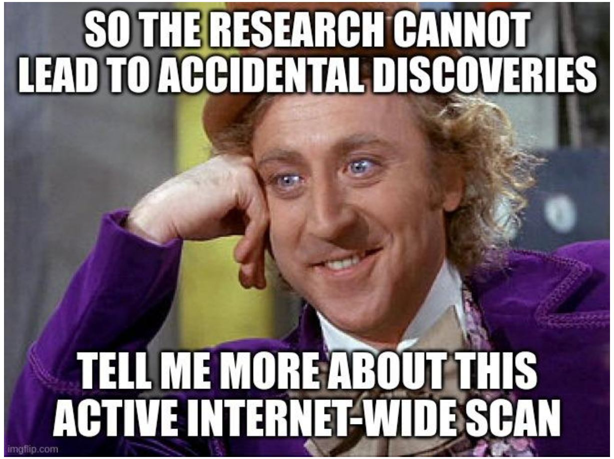
How to pose questions?

Clear and concise

- Researchers will not read ethics papers && disregards long questionnaires

Each question is indicative of multiple risks

Risks (in-)directly covered by more than one question


SO THE RESEARCH CANNOT LEAD TO ACCIDENTAL DISCOVERIES
TELL ME MORE ABOUT THIS ACTIVE INTERNET-WIDE SCAN
imgflip.com

Our CybSec questionnaire

Will the research involve any cybersecurity or online privacy issues, such as [...], or the discovery of illegal activities on the Internet?

Q1 Security Weaknesses

Q2 Malicious Software

Q3 Internet Scan

Q4 Accidental Discovery

Q5 Coordinated Vulnerability Disclosure

Questions-risks mapping

	Q1 Security Weaknesses	**Q2** Malicious Software	**Q3** Internet Scan	**Q4** Accidental Discovery	**Q5** Vulnerability Disclosure
R1 Accidental discovery	●		●	●	●
R2 Publication of private data	●		●		●
R3 Damaging production systems		●	●		
R4 Misuse by malicious actors	●	●			
R5 Discovering vulnerabilities	●		●		●
R6 Reprisal against researcher	●			●	●
R7 Lack of consent		●	●	●	
R8 Damaging people or companies			●	●	
R9 Illegal behavior by researcher		●	●		

Coordinated Vulnerability Disclosure (CVD)

https://addxorrol.blogspot.com/2019/08/rashomon-of-disclosure.html

Our procedure & guidelines

Write up findings && immediately report to the responsible party

Expect the affected party to respond within 21 days

If no reply, explain publication timeline and give another opportunity to get in touch

If no fix is available after 90 days

- Consider disclosing the vulnerabilities publicly
- Be willing to negotiate publication date

CVD: Reporting

Make a reasonable effort to find the right contact for reporting a vulnerability

Make sure to use a secure channel before including technical and confidential details

Contact software distributors in case of no reply from vendors

When necessary, we request assistance from the NCSC-NL and DIVD

CVD: Disclosure

If no fix is available at the end of the agreed publication date (e.g., after 90 days)

- Notify again the intent to disclose the issue

Disclosure paths depend on the nature of the problem

Evaluate each issue on a *case-by-case basis* based on the *risk to people*

Include a timeline to report communication & remediation actions taken by parties

CVD Procedure as a University Policy

We are working to make the procedure part of an official University Policy

- Clear to researchers how they are expected to behave
- Leverage in demanding that researchers follow these procedures
- Provides researchers with assurance that they will be protected
- Clear to recipients of disclosure notices how we handle the process

What’s next?

- Iterate over questionnaire and keep it up to date
- Teach these topics to students
- Scalability challenge of our CVD procedure

Conclusions

- Ethics issues in CybSec research are *not only related to human subjects*
- Critical to have *domain-specific experts* in Ethics Review Boards
  - Also, having an ethics philosophy specialist
- *Practical guidelines & questionnaire* for ethics review of cybsec research

https://www.utwente.nl/en/eemcs/research/ethics/

Disclaimer: We want to inspire others to follow similar approaches, not to strictly define global rules

Thanks!
Questions?

Andrea Continella
<a.continella@utwente.nl>
https://conand.me
🐦 @_conand

Practical Steps

Findings must be immediately reported to the supervisor/teacher

- Supervisor/teacher takes responsibility for handling the disclosure
- Explain that this was done in scientific environment/research
- Be willing to negotiate publication date, pending response/remediation actions
- Still have a (negotiable) deadline (to prevent deadlock because of no response)
- Make sure this is written in a friendly, open tone
- Discuss and work with the affected party to design and test mitigation and fixes