Seminar 1 – Ethics in Cybersecurity research and practice

The authors are raising the concept of ethical awareness and they are emphasizing the importance of having a deeper and more nuanced understanding of ethics within the cybersecurity field. Ultimately, they want to accelerate the tuition of ethics in computer science education, the development of effective code of conducts, and the discussion of ethics in cybersecurity.

The recommendations presented in this paper may be fuzzy considering that cybersecurity is a rather new, unexploited, interdisciplinary, and complex field with a not ending amount of technical arrangements. Personally, I am sure that most readers of this article would agree on the overall recommendations and conclusions presented by the authors. That we in general need to raise and highlight ethical awareness, and that we in the future want to develop clearer and effective code of conducts. However, I think that most of the “grey zones” would persist due to the nature of the interdisciplinary and complex field and that ethics are already discussed in education and research even more than for just 5 years ago. One would have to accept that e.g. code of conduct will take time to develop and that it cannot be compared to the medical industry.

**Case Study 1 – Academia (Research)**

The paper brings up the research project case “Encore” where the level of censorship was measured through a web client script requesting a set of multiple websites which were considered “less controversary”. The script was loaded into a bunch of servers and was spread (unknowingly) to clients accessing those servers. When the response was captured to the set of websites, the result was sent back to the script creators. The researchers did not ask for consent with motivations including that there are certain classes of experiment which does not require informed consent, such as when obtaining consent is either prohibitive, impractical and there is little appreciable risk of harm to the subjects. They also argued that asking for consent would be a burden and reflect bad on the result. The researchers did however recognize some ethical issues and the measurement collection was sent for reviewing by 2 recognized REBs but was declined as it did not manage Personally Identifiable Information (PII). Ultimately, the experiment was at the time “outside of everyone’s responsibility” and performed, and the potential harm became huge due to the fact that an individual within an regime could’ve sent the request to banned sites and draw a secret service attention etc.

**Case Study 1 – Issues**

This case demonstrates a lack of ethical awareness of both the researchers and the research ethics boards that the research collection data was sent to. It demonstrates that informed consent may become expensive for researchers and that a balance between the research result and the potential harm is very important. The case demonstrates that a research result today may ethically justify the potential harm for research subjects. Along with the lack of ethical guidance, ethical awareness, and the complex field of cyber security, we may encounter many gray zones and many situations where actions and research may be out of everyone’s responsibility and remain unsettled. A clear problem in this case is that the danger of this research should have been identified both by the researchers and the REBs, and thus be defended by an institutional ethics policy.

**Case Study 2 – Practitioner community (industry)**

An independent research group purchased and attacked medical devices including pacemakers and heart monitoring devices, from the company St. Jude Medical. They claimed to find multiple vulnerabilities in the gear, but instead of disclosing this to St. Jude Medical directly, the group teamed up with the investment firm Muddy Waters to short its stock. Another research group claimed not to find any vulnerabilities, a third group agreed that there were some vulnerabilities in the St Jude systems. Initially, the MedSec group did not make any significant profit on the short and St. Jude Medical denied the claims and performed a lawsuit against MedSec. Eventually, MedSec got right and 465,000 pacemakers were recalled. Ultimately, St. Jude Medical denied the claims and thus responsibility, MedSec claimed that their cooperation’s with Muddy Waters were the fastest route due to St. Jude Medicals poor history of responding to security flaws.

**Case Study 2 – Issues**

This case brings up many questionable ethical issues.

**Takeaways**

As methods of ethical oversight, the authors present the Menlo report, the Association of Internet Research guidelines, Oxford Internet Institute - Networked Systems Ethics guidelines, code of conduct (institutional and corporate), research ethics boards (academic), policies (institutional and corporate).

Ethical issues arising in academic contexts:

* Respect for persons
  + Informed consent
* Beneficence
  + Protection of subjects from inadvertent harm
  + Privacy
  + Reporting incidental findings
  + Testing the security of the system
* Justice
  + Bias
* Respect for law and public interest
  + Coordinated vulnerability disclosure
  + Testing on live and sensitive systems
  + Impact on the commercial viability of a system
* Recognizing ethical issues
* Competence of REBs

Ethical issues arising in practitioner industry:

* Respect for persons
  + Informed consent
  + Trust
* Beneficence
  + Privacy and control of data
  + Risk
  + Security
* Justice
  + Bias
  + Responsibility
* Respect for law and public interest
  + Vulnerability disclosure
  + Business ethics

**Questions**

Do you think that a code of conduct like the one in medicine can be developed in nearest future?

Do you think that we shall integrate more ethics in computer science education?

Do you think that the public disclosure by MedSec is justified for a quicker patch of the medical equipment?