Seminar 1 – Ethics in Cybersecurity research and practice

**Case 1 - Academic research (Encore)**

The level of censorship was measures through a script spread through servers to clients. The script performed requests to certain sites without the knowledge of the subjects and the response was sent back to the script creators forming the research data. The researchers recognized some ethical problems (controversial site were left out, widely known, and accepted website were requested) but built up a defense against not asking for consent.

The data collection was sent to REBs of 2 leading universities, but they refused to review it due to the lack of PII. Along with a lack of ethical awareness and a drive to include certain data, this resulted in a large potential harm for subject (There could be subject in e.g. regimes where certain activity is flagged for secret service agents and such, making them a target).

Ultimately, the research had the potential of harming multiple individuals. But the harm was not fully recognized and accounted for due to the “gray zone”, lack of ethical awareness, lack of informed consent and the faulty judgment done by the 2 REBs.

**Case 1 – Takeaway**

It seems that the researchers missed an important ethical consideration or that they thought that the result would justify the means and that the potential harm was overlooked to ease the research. There seem to be no consequence of taking this risk, not until know when flagged and warned by SIGCOM’s program committee and this article.

Along with unclear guidance and policies, this research ‘fell in-between’ and were ‘out of everyone’s responsibility’ due to a lack of ethical awareness of the researchers, IRB and REB’s. This case demonstrates that in new cybersecurity research, there may be ethical issues that one has never encountered before. These issues are left for interpretation by the researchers if these are not presented to or understood by REBs.

**Case 2 - Practitioner field (MedSec, MuddyWaters vs. St. Jude Medical)**

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. 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, another research group claimed not to find any vulnerabilities, a third group agreed that there were some vulnerabilities in the St Jude systems. MedSec got right and 465,000 pacemakers were recalled. 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 2 – Takeaway**

This case brings up many questions regarding legal responsibilities, social responsibilities, and ethical responsibilities. At the same time, it is also a balance of legal, social, ethical, and financial rights. MedSec could be accused of leveraging the vulnerability for a financial benefit and for exposing the users of St. Jude Medical’ gear to potential harm. St. Jude Medical could be accused of not managing the vulnerability disclosed, delaying a security patch, or not compensating the researchers.

**Takeaways (Methods)**

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).

**Article – Review**

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 would agree on the overall recommendations and conclusions presented. 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.

**Questions**

* Do you think that an effective code of conduct like the one in medicine can be developed in the nearest future for cybersecurity?
* 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?
* Do you think that the data collection in Encore would be sufficient enough if informed consent would be implemented?