Seminar 1 – Ethics in Cybersecurity research and practice

## Summary

Focus on cyber security. Presents 2 case studies, one about some ethical issues facing researches in the cybersecurity and the other highlighting shortfalls in governance practice.

There is a lack of oversight regarding cyber-security ethics. In the university-based development: Lack of awareness as to the nature of the ethical problems regardning cyber-security.

In the broader community of practicing cybersecurity experts, problems are widely known but there are a lack of adequate guidance or accountability form a barrier to consistent ethical practice.

## General

The paper critizes cyber-security ethics by providing an overview of some of the ethical issues in 2 case studies.

* Case Study 1 (Issues facing researchers in the cybersecurity community)
  + Academic research community
    - Can rely on research ethics boards (REBs)
* Case Study 2 (Shortfalls in governance practice)
  + Corporate practitioner community
    - REBs are typically unavailable for this community.

Conclusion: Ethics shall be taught in far greater depth on computer science courses. Code of conduct shall be developed and deployed provided they are effective. An active discussion about the topic “ethics in cybersecurity and cybersecurity research” is needed.

They mention “current methods”, what methods are there?

Methods fail in:

* University-based development (lack of awareness in the community)
* Broader community of practicing cybersecurity experts (lack of guidance and a barrier of accountability)

They make a point:

* Cybersecurity ethical problems go largely ungoverened and unguided despite the potential for significant harm.

Proposal:

* Need to be a greater appreciation of the risks of cyber security development in ethical review committees and clear code of conduct for the professional community which cover both development and practice.

Case with Encore solution:

* Unethical but, despite this sought for approval of the ethics committee.

## Case study 1

A paper on an experiment (or research) on censorship, specifically monitoring levels of censorships.

* Scripts were placed on the webservers of obliging companies and was seamlessly transferred to the computer of clients visiting those webservers.
* From the clients, Encore would then try to access sites that were likely to be censored and send information about their success or lack, back to the script designers.
* Clients were not aware that Encore was running on their machines.
* Clients were not asked for consent.
* Basically the whole world were ultimately targeted.
* People may have been highlighted by secret services due to, through the script, access to websites with a high likely-hood of being censored.
* Due to such problems and that the access in this case could be, by the secret services, related to people’s fight for free speech, the requests made by the Encore could potential result in severe harm.
* Authors did not recognize some of the ethical concerns with their work.
* The measurement collection was not reviewed by the REB’s because it did not collect or analyse Personal Identifiable Information (PII) and was not human subjects research.
* The report references the Nuremburg Trials which direction much of contemporary research ethics is founded upon.
* Experiments can be conducted ethically without consent if there is a little appreciable risk of harm to the subject, when obtaining consent is either prohibitive or impractical.
* However, this study does not seem to be a case of where collecting consent would be prohibitive nor a classification of low-risk observation.
* They argued that the task of requesting informed consent would be to complex due to the explaining of technical concepts and language barriers.
* The authors of the Encore notes further than informed consent does not decrease risk for subject, it only alleviates the researrchers from some responsibility for that risk and may even increase risk to user by removing any trace of plausible deniability, for the report authors that’s a post-hoc justification.

## Ethical issues arising in academic contexts

A summary of experienced issues (academic) are presented according to Menlo principles:

* Authors of the report concludes that the take-up of the Menlo-principles (2012) has been slow. Since the Encore case was brought up 3 years after (2015).

Menlo report (4 principles for ethical research)

* Respect for persons, beneficence, justice and respect for law and public interest)

Stated problem:

* The issues in ethics within cybersecurity do not easy fit within the Menlo framework.

List:

### Respect for persons

Voluntary, informed consent, individuals with diminished autonomy, incapable of decding for themselves, are entitled protection.

### Informed consent

Back-bone of research ethics, Ability to and act of gaining informed consent from those being affected by the research.

### Beneficence

Systematically assess both risk of harm and benefit. Max probable benefit, min probable harm.

### Protection of subjects from inadvertent harm

Unintended harm is still harm. The principle of minimization of harm to the participant overrides the interest of the research, particularly, in cases where little or no consent has been given.

### Privacy

Privacy issues arise in cybersecurity. Legal sensitivity is markedly varied. Data of individuals in America, Asia or Africa are far less subject to regulation. Could cause problems in research – That research as dumped to other countries due to “better” data.

### Reporting incidental findings

Decisions need to be made in advance as to inform an entity if appropriate. I fno policy is written in advance, ethical dilemmas may arise.

### Testing the security of a system

Researchers may need to act like a malicious party, identify and use vulnerabilities in order to fully test a system. Where avoidance of harm is not possible an ethics committee can be beneficial.

### Justice

Each person deserves equal consideration in how to be treated..

### Bias

Example: Encore project. Researchers in West may have little experience of less advantages groups living elsewhere in the world leading to inadvertent bias agains those groups. Prallell between automated systems and cybersecurity.

### Respect for Law and public interest

Be transparent in methods and results, be accountable etc

### Coordinated vulnerability disclosure

Important consideration – Shall incidental vulnerabilities be planned for and alleviated to a pertinent authority etc? Could protect all involved, also the researcher since it could solve problems in cases where no informed consent was obtained.

### Testing on line and sensitive systems

Redundancy systems, critical national infrastructure etc

### Impact on the commercial viability of a system

Do the researcher have a whistle’blower duty to make e.g. unpatched vulnerabilities public etc.

### Recognizing ethical problems

Again in the TOR network research, researchers were not assessed to violate any of the universitie’s thics policies since the work was not classifiable as human subject research.

### Competence of REBs

Conslusion: REBs tend to react to well-recognized etchical and legal problems such as privacy and related issues regarding personally identifiable information but not to other fields or more complex fields of cybersecurity with the need of both computer science and ethical backgrounds.

Most REBs consists of ethics experts without knowledge and experience of computer science research and research methods. Aswell as computer science researchers lack in ethics knowledge.

## Summary Case 1

The lack of knowledge and experience of computer science combined with ethics must be changed from the base (elementary programs) to make an impact on the research ethics oversight. There are a lot of fields within the cyber security research not making a standard part in Universities and REBs ethics policies and regulations.

## Case Study 2

About MedSec / An independent security research group. They tried to attack a number of St/ Jude Medical devices, including pacemakers and heart monitoring device designed for home usage.

Muddy Water – Investment company teaming up with MedSec for shortening the St Jude medical equipment.

Should MedSec have partnered with an investment company to short the stock of a company it knew would suffer on the market once the flaws were made known?

Should cybersecurity researchers be protected from legal action such as the attempt to sue MedSec pursued by St Jude?

* Answers are unclear in both cases…

Problems from the

* Penentration testers perspective
* Researchers should be protected from predatory practices by companies seeking to paper over cracks in their own security through legal action.
* Medical company or hospital perspective
* Investment company perspective.

Report authors suggests a code of conduct.

Listed ethical issues in practice:

### Summary of the issues

Many of the issues are similar to the one in the academia, but they are frequently complicated by a lack of institutional tradition and policy governing behavior, an absence of REBs, and conflicts of interest between making money and doing “the right thing”.

Cybersecurity practice is broken down into four broad areas inline with the Menlo principles: Respect for persons, beneficence, justice and respect for law and public interest. ‘

### Respect for persons

### Informed consent

Same problems as the academia. In many cases there may be effectively impossible to obtain informed consent. Some groups have by tradition of not seeking informed consent which makes it difficult for a conscientious cybersecurity practitioner operating in these fields to insists on obtaining one.

### Trust

Build relationship between the security and those being secured. Increase transparicy and access to cybersecurity teams.

### Beneficence

### Privacy and control of data

Example – Facebook and Cambridge Analytica was not a question about privacy, but a question of what was done with peoples data and sharing of that data without consent. Example. If researching for potential vulnerabilities in 2 connected networks, then exploring a vulnerability in one may lead the researcher into the connected network and through that to personal data unintentionally.

### Risk

What are acceptable risk thresholds, who is taking the decisions, who is affected by them, how is risk calculated? Cost vs risk decisions involves many ethical issues.. Argue for a greater level of diversity in the decision-making process.

### Security

Many examples of ethical issues: Compromises of security through insufficient funcing, poor oversight of systems, late or no installations of pacehs, how and where data is stored, ho data I s accessed, poor training in staff in security awareness.

Training, priorities, more budget, involve the cybersecurity team from the start of the development process.

### Justice

### Bias

Diverse composition of cybersecurity team members.

### Responsibility

Example: To what degree shall the state protect its own economy on the internet as it does in physical space? Should a company be responsible for developing its own cybersecurity?

### Respect for law and public interest

### Vulnerability disclosure

When breaches occur, should these be reported and to whom? Sharing information about a vulnerability is increasing that vulnerability unless it is controlled. On the other hand, pooling experience might be the only way an effective defence can be mounted.

Convention, but conventions can be used.

When and how can be disclose a vulnerability? To protect researcher, subject and the object?

### Business ethics

Loog up the Equifax breach. Insider trade. Many parties interest.. Making money..

MedSoft was not a matter of insider trading, but they could have contacted St Jude to give them time to patch the problem. Another example is the CEO of Yahoo, who did not inform the public of the hacks in 2013 and 2014 regarding accounts.

## Existing guidelines and recommendations

Little guidance in cybersecurity practitioning.

There are guidelines for ethical research from the Association of Internet Research, but these are seen as series of questions to reflect about rather than principles for guiding conduct.

The controversary surrounding Encore arose in large part due to the networking research community does not yet have widely accepted guidelines or urules for ethics of some experiments.

IEEE and ACM (institutional level) or corporate level have developed code of conducts .

Menlo principles mainly for cybersecurity but very broad.

Codes must be supported by effective sanctions.

A support system for a type of code of conduct similar to the one in medicine does not exist in the field of cyber security.

Professional bodies like IEE and ACM could also look to provide research ethics recommendations for members.

A development of an active conversation about cybersecurity ethics both in research and in practice is needed.

Traction for teaching ethics in computer science in general and cybersecurioty in particular is needed.

### Conclusion

Methods of oversight and guidance of cybersecurity are inadequate in both areas: university-based development and the community of practicing experts.

Academia:

* Lack of awareness among members and thical review committee

Practicing:

* Lack of adequate guidance or accountability build a barrier to consistent ethical practice.

There needs to be a greater appreciation of the risks of cybersecurity development in academic ethical review committees and clear codes of conduct for the professional community which covers development and practice.