Seminar: The Computer Engineer's Code of Ethics

Daniel Bosk

Department of Information and Communication Systems
Mid Sweden University, Sundsvall

1 Introduction

Considering that our world becomes increasingly dependent on computer systems, it is important that those of us who are capable of controlling the computer systems do this in a responsible way. But what is a responsible way? This is the topic of ethics, the reasoning about moral obligations. There are a great many texts written on the subject, we will in this assignment study some of the lighter ones.

As an example, since our digital world allows the copying of information more easily, more people do this. This can happen in the form of people using a service for publishing photographs to friends, or to the entire world for that matter. Sometimes the consequences of this can be severe. For instance, when a child posted vacation pictures to Instagram [9]. This happened to be not any child, it was the child in the Norwegian royal family. These images posted, did due to our technical development, contain the exact GPS coordinates of the location where the picture was taken. The result being that the position of the royal family was published in almost real-time, information which is normally strictly secret.

This is also an issue for non-celebrities. And the question is, where ends the responsibility of the engineers who contributed to these systems? Should they be morally obliged to ensure the user can make an informed choice? Or is that totally the responsibility of the user? What if the design does not let the user make an informed choice?

We can then step it up a notch. In app stores, e.g. Google Play, there are occasionally apps found which performs some morally questionable activities. An Android app, "Brightest Flashlight" by Goldenshores Technologies, which could be found for free in the Play store, gathered data on users' locations and device identifiers, which the company later sold to advertisers [5].

Another, more draconian, example concerns manufacturers of surveillance equipment, selling this equipment to authoritarian regimes for purposes of surveillance, censoring and in general repressing the people, as is the case for the companies Narus, BlueCoat Systems, Trovicor and Cisco [4]. Narus sold equipment used for surveillance to the Egyptian government. BlueCoat's equipment was used in Syria. Germany-based Trovicor sold their technology to Bahrain; "dozens of activists were tortured before and after being shown transcripts of their text messages and phone conversations captured from this technology" [4].

Is this type of engineering anywhere near ethically defensible?

2 Aims

This seminar aims to discuss the ethical issues regarding the problems described above, i.e. the moral responsibility of engineers. After doing this assignment your should be able to:

- Value and argue about different ethical aspects of computer security, e.g. possibilities for surveillance, and its consequences in society.

3 Reading

This assignment is based on the Codes of Ethics of two engineering associations. Thus, before you start you must read *Code of Ethics: ACM Code of Ethics and Professional Conduct* [1], *Software Engineering Code of Ethics and Professional Practice* [2], and finally *IEEE Code of Ethics* [3].

Once you have read this you should read two articles analysing Snowden's revelations about the NSA surveillance techniques. The first one is "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations" [7]. The second one is "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations" [6]. Finally, in your favourite search engine, search for the string

"nsa exploit of the day site:www.schneier.com".

Read about a few of the NSA exploits presented there.

Lastly, you should read about the "famous" Apple versus FBI case, where FBI wants Apple to engineer a weakened version of iOS so the FBI can break its security. In particular you should read the article "Apple engineers rebel, refuse to work on iOS amid FBI iPhone battle" [8].

4 Assignment

The first thing you should do is to analyse the cases presented in the texts you have read, i.e. the NSA's mass surveillance and FBI's wish for Apple to weaken the security of its products for the FBI. You should analyse them from the perspective of the codes of ethics that you have read: which parts are "right" and which are "wrong"? Are there conflicts? Make sure to write down your conclusions and motivations.

You are now going to position yourself as one of the engineers working for the NSA or Apple. Prepare a document with two parts. The first part should contain arguments for why you should develop these exploits or intentionally weaken security, the second should contain arguments against developing these. Your arguments should have their base in the codes of ethics you have read (include references), but also your own ethical values may be used in your argumentation — but make sure to note when they conflict!

During the seminar, discuss your analyses and your positions.

5 Examination

This assignment is examined through active participation in a seminar and a hand-in. To prepare for this seminar, follow the instructions in section 4. Hand in the resulting document (analysis of the cases, your position) in the course platform and also bring them to the seminar. Then you attend the seminar, see the schedule. You must participate actively to pass this assignment.

References

[1] Association for Computing Machinery. *Code of Ethics: ACM Code of Ethics and Professional Conduct*. Accessed on 4 April 2014. URL: https://www.acm.org/about/code-of-ethics.

[2] Association for Computing Machinery. *Software Engineering Code of Ethics and Professional Practice*. Accessed on 4 April 2014. URL: https://www.acm.org/about/se-code.

[3] Institute of Electrical and Electronics Engineers. *IEEE Code of Ethics*. Accessed on 4 April 2014. URL: http://www.ieee.org/about/corporate/governance/p7-8.html.

[4] Electronic Frontier Foundation. *Mass Surveillance Technologies*. Accessed 4 April 2014. URL: https://www.eff.org/issues/mass-surveillance-technologies.

[5] Lee Garber. "Security, Privacy, Policy, and Dependability Roundup". In: *IEEE Security & Privacy* 12.1 (2014), pp. 9–10. ISSN: 1540-7993. DOI: 10.1109/MSP.2014.13.

[6] Susan Landau. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations". In: *IEEE Security & Privacy* 12.1 (2014), pp. 62–64. ISSN: 1540-7993. DOI: 10.1109/MSP.2013.161.

[7] Susan Landau. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations". In: *IEEE Security & Privacy* 11.4 (2013), pp. 54–63. ISSN: 1540-7993. DOI: 10.1109/MSP.2013.90.

[8] Shaun Nichols. "Apple engineers rebel, refuse to work on iOS amid FBI iPhone battle". In: *The Register* (Mar. 2016). URL: http://www.theregister.co.uk/2016/03/18/apple_fighting_fbi_demand/.

[9] Paul Roberts. *Wayward Instagram account creates security scare for Norwegian Royal family*. Aug. 2012. URL: http://nakedsecurity.sophos.com/2012/08/23/instagram-norway-royals/.