Ethics of the Vulnerability Research and Penetration Testing

One can easily find weak points and vulnerabilities virtually everywhere: our bodies are vulnerable to viruses and weak in front of the eternity, and there's a lot of weak points in our memory and our mind. All the software solutions we create are also imperfect.

In this article, I will try to address matters related to the ethics of the vulnerability research and pentesing.

It seems that the humanity was trying to find vulnerable points in each sphere of life. In medicine, for example, doctors are examining the body of a dead person in order to understand the key principles of the human body, as well as to get the idea about its inner structure.

In my opinion, the history of medicine and the history of software vulnerabilities research and exploration have a lot in common. Just a couple of dozen years ago medical scientists could be easily blamed for their studies because such work was strictly prohibited by the ideology of the ecclesiastical state. While the time was passing by, the humanity realized the need for medical studies and experiments and created a set of specific rules and recommendations for such things. For example, Nuremberg Code or The Belmont Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research.

It's simply impossible to imagine our modern lives without the information technologies. They are integrated into all aspects and fields of our day-to-day routine. However, all technologies have their own vulnerabilities, which carry a serious threat to the human.

Now let's define two key terms – the ethics and the vulnerability:

Ethics is the branch of knowledge that deals with moral principles, their developments, as well as implementation in the society.
The vulnerability is a parameter characterizing the possibility of applying damage of any nature to the system described by some external means or factors.

Why do we need to find vulnerabilities?

There's a wide range of situations when one needs to search for vulnerabilities, here are some of them:

— curiosity
— research interest
— vested interest
— the desire to be famous and gain reputation
— a whole range of personal motives
— doing a good deed

There's an interesting situation from the standpoint of ethics when a person has all required knowledge and skills to search for vulnerabilities, but avoid doing that until he faces extremely compelling circumstances.

In order to find the right answer to this question, I want to offer you a slightly changed Heinz's dilemma:

Imagine that a woman suffers from a specific form of cancer. There’s only one drug that can save her life. This drug was invented just a couple of years ago and the production cost is incredibly high. In addition, the pharmaceutical company decided to sell it 10 times more than it costs to produce the drug.

The husband of the affected woman, Mister Heinz, visited all his friends and relatives in order to collect some money. He also used all legal ways to get money but managed to collect only a half of the required amount. He addressed the pharmaceutical company and the management to reduce the price or offer him an installment plan. The company refused to make any changes to their pricing policy.

That was the moment when Mister Heinz decided to hack their corporate network, steal the secret formula and production technique, and give that information to someone, who could produce the drug and sell him at a lower price.

- Should Mister Heinz steal the medicine formula and why?
- Would Mister Heinz have been obliged to steal the medicine, if he hadn’t loved his wife?
- Let’s imagine that the affected woman is not his wife. Should Mister Heinz steal the formula for someone else?

The most important thing is that there’s no right solution to this dilemma. If a person believes that a pharmaceutical company needs to be hacked, it cannot be called more moral or less moral. The whole question is how decisions are made.

I find the opinion of Bruce Schneier in this case really interesting:

To me, the question isn't whether it's ethical to do vulnerability research. If someone has the skill to analyze and provide better insights into the problem, the question is whether it is ethical for him not to do vulnerability research.

Probably, one can partially agree with the above opinion that the central question is not whether to investigate or not to investigate the software for vulnerabilities, but how ethical it is for a given researcher to carry out such work, can he conduct such studies, and how ethical the research is, and of course there is a question of the applicability of the law.

What are the codes of ethics in the field of IT?

— IEEE Code of Ethics
— Software Engineering Code of Ethics
— ACM Code of Ethics and Professional Conduct

Key principles of the ethical vulnerability research

According to the authors of Empirical Research and Research Ethics in Information Security article, the following principles should be used as the foundation for the ethical vulnerability research in the field of information security:

— Do not harm humans actively

— Do not conduct undercover research
— Do not watch bad things happening
— Do not perform illegal activities to harm illegal activities

The Australian Council for International Development offers the list of 10 questions, which have to be answered before starting any research:

1. Is the research necessary and well justified? What are you looking to investigate and why is it important?
2. Is the research well planned? Does it connect to a particular program of work in your organization? Do researchers have the relevant expertise to conduct the research?
3. What is the context in which the research will be conducted? How will this context influence the research design?
4. How is the methodology and analysis appropriate to the context and what is being investigated?
5. What are the potential harms and benefits for researchers and participants that could arise from the research?
6. What information about the research will be provided to the participants? How will free and informed consent be obtained and ensured throughout the research process?
7. Are there any other parties or partners involved in the research? What are their interests in the research? Who will benefit directly and indirectly from the research?
8. How do you plan to protect confidentiality and anonymity? What will happen to the data? How will it be accessed and secured?
9. Have researchers received training, information, and assistance related to addressing ethical issues?
10. How will the findings be disseminated and used? Will participants have access to validating and receiving the results of the research? What will happen when the research is complete?

It’s worth listing a couple of question from one more paper called Towards Community Standards for Ethical Behavior in Computer Security Research:

— Are the research results intended to protect a specific population, and if so, which population? (E.g., the owners of infected hosts, the victims of secondary attacks using a botnet, the researchers’ own institution, or the general internet user.)
— Is there a way to achieve multiple benefits to society simultaneously when studying criminal botnet behavior? (E.g., developing new defenses, while aiding investigation of criminal acts and assisting victimized network sites?)
— Who will benefit more from the publication of research findings, and in which order: Victims of criminal acts; authorities responsible for protecting their citizens; the researchers themselves; or the criminals who are perpetrating computer crimes?
— Is there any other way to accomplish the desired research result(s)?

Conclusions and propositions

Analyzing all the information above we can say that there’re at least two main categories of questions and issues that have to be addressed.

Ethics of the researcher

Before starting any work, the researcher has to answer a simple question: *“Will I do any harm?”* No doubt that any interface of a working technological system that has access to the World Wide Web will become a subject of research. Any pentest may cause a short suspension of production or may result in a catastrophe.

The second important question is the *conflict of interests* of the researcher. It’s recommended to avoid performing any pentests in case the researcher is interested in a specific outcome of the study. For example, a famous information security expert is performing the security audit of the company, while a close relative of the expert owns a share in this organization. The personal interest of the information security expert is clear and obvious.

Another important thing is *privacy*. The information obtained by the researcher shouldn’t be used for personal advantage or in any other unlawful way.

The fourth important aspect is *professionalism,* i.e. the level of competence of the researcher in the field of vulnerability research. For example, who has more ethical rights – a first-grade student of a technical university, or an information security specialist with five years of experience.

I think that we need an independent evaluation institution which may "score" candidates. After all, no one allows a student studying to become a surgeon to operate patients without necessary experience working at least as a surgeon's assistant.

Research ethics

Talking about the research itself, I think that we need to consider the following points:

- *Research goal* – one needs to understand if the goal corresponds to the main ethical principles. For example, it’s hard to consider ethical a research of the cardiostimulator safety, when the researcher clearly understands that the main goal is to increase the market price of the corporate shares in order to get profits and cover expenses for such research. Listen to the interview with MedSec Holdings CEO, Justine Bone.
- *Research scope* – the researcher must understand what should be tested and what not.
- *Research methodology* – carefully selected methods should allow reaching the goals of the research.
- *Research privacy and security*– if the bad guys may get their hands on even a part of the information received during the pentest, this may cause a lot of problems.
- And the most important question: *Does the research infringe the human right of personal privacy and safety?* Obviously, after getting information about the vulnerability of the cardiostimulators, their owner won’t stay indifferent. At the very same time, it’s simply impossible to prohibit such information from spreading

Keeping all this in mind, I can offer the following checklist for any type of vulnerability research:

1. Is this research really worth it? What are pros and cons?
2. What is the real goal of the research?
3. In case you work in the field of information security, do the goals of the research correspond to the goals of the company?
4. Do researchers have the appropriate knowledge to conduct the pentest?
5. Does the methodology correspond to the inner structure of the research?
6. Is there any other way to obtain similar results?
7. What are the potential harm and profit for researchers and the participants at the end of the research?
8. Are there any other parties participating in the research? What are their interests? Who will benefit (directly or indirectly) from the research?
9. Is there any conflict of interests related to the research?
10. How do you plan to protect the privacy and the security of the found data?

11. Do researchers have any training or experience related to solving ethical issues?

Numerous ethical questions related to the research and exploration will always be here. According to the history of medicine, we need to create a public institution in order to control the process of vulnerabilities research and exploration in the field of IT. I want to hope that the social understanding of the vulnerability research will only develop. We can see some slow development in the field of the disclosure of the information related to vulnerabilities already now.

Resources:

- https://history.nih.gov/research/downloads/nuremberg.pdf
- https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html
- https://www.schneier.com/essays/archives/2008/05/the_ethics_of_vulner.html
- https://www.ieee.org/about/corporate/governance/p7-8.html
- https://www.computer.org/web/education/code-of-ethics
- https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct
- https://macsecurity.net/
- https://acfid.asn.au/sites/site.acfid/files/resource_document/ACFID_RDI%20Principles%20and%20Guidelines%20for%20ethical%20research12-07-2017.pdf
- https://www.bloomberg.com/news/videos/2016-08-25/medsec-s-bone-hope-st-jude-responds-with-urgency