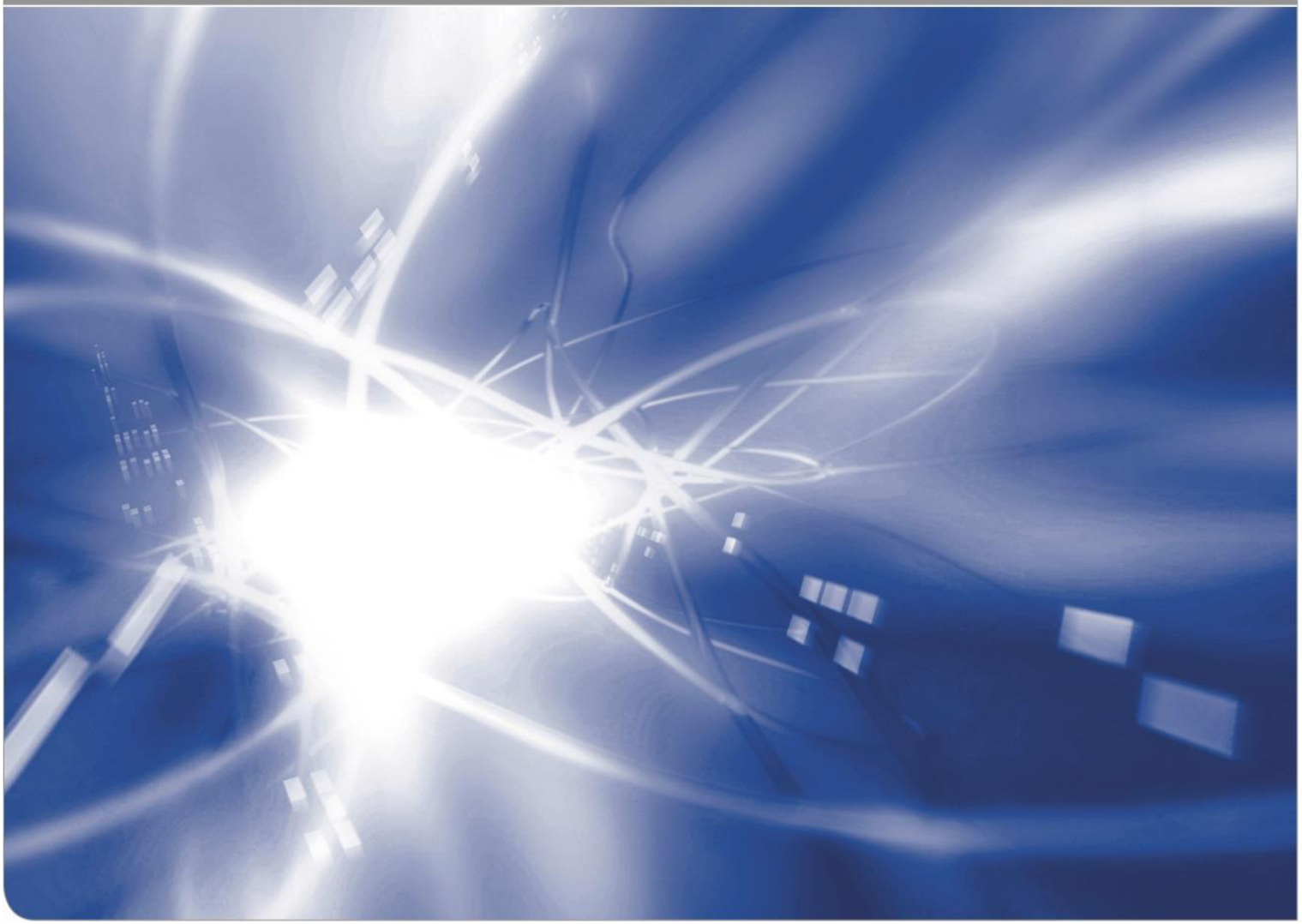
Karlsruhe Institute of Technology

The Art of Hacking

by Miriam Ommeln, Lexi Pimenidis

KIT SCIENTIFIC WORKING PAPERS 83



This paper was finished in 2009 and is a slightly modified version of our German paper '*Kunstfreiheit statt Hackerparagraph*',which was published at the *26th Chaos Communication Congress* (26C3) by the Chaos Computer Club.

Impressum

Karlsruher Institut für Technologie (KIT)
www.kit.edu

2018

ISSN: 2194-1629

The Art of Hacking

Miriam Ommeln and Lexi Pimenidis

ABSTRACT

In this position paper we will try to take up on the discussion of *ethical issues* and *hacking*. In this work we would like to show what actually happens during hacking and how hacking relates to social responsibility, directed at the benefit of our society. This discussion is necessary for legal discourses and future ethical codices. We come to the conclusion that the discussion actually resolves to *aesthetic* instead of ethical questions. The latter are only an artificial addendum. However, if hacking is related to art, hackers should receive the same degrees of freedom as artists. In consequence, we would like to suggest to put the *right of freedom of the arts,* called *Kunstfreiheit* in Germanic countries, into effect for hackers too.

KEYWORDS

IT-Security, Hacker Ethic, the Art of Hacking, the Right of Freedom of the Arts (Kunstfreiheit)

1. INTROCUTION

"The world wants to be deceived" and "Everybody is a lier" are two of the eldest proverbs.[1] Both seem to be within the credo of a modern hacker.[2] However, another legal principle which holds today is *audiatur et altera pars*, i.e., no person should be condemned unheard.[3] On the other hand, the democratic social order bases on Thomas Hobbes and his remarkable assumption of a *war of every man, against every man*[4]. Similarly, modern security politic is unquestionably guided by the principle of *If you wish for peace, prepare for war*[5].

But who are the two extremes to be heard? Classical, i.e., defense base IT security research on one hand and hacking on the other hand are not disjoint areas *per se*, as *Les extrêmes se touchent.*[6] . To a certain degree the line between both disciplines is blurred, hence the question rises to which extend ethical discourses can be considered a suitable tool and applicable in our case. The main reason for *not* applying ethical arguments for discourses like "ethics and hacking" or "ethics in IT security" is that it can become a tool to measure itself. How should a tool be able to criticise itself when it can use only itself for the critique?

In this scenario of social-, power-and economic-political interests it is too easy to reach the point where *during war, laws are silent* and also *the rigor of the law is the height of oppression*.[7] Traditional ethical approaches using descriptive or normative tools, e.g., empirical considerations or case studies, are not suitable in our case of extreme interferences with regards to *good* and *bad.*

In our case, applied ethics can show nothing more that, other than legal privileges, morale can neither been forced, nor claimed appellatively[8] – even if the legal system is flexible. In the global context of

[1] "Mundus vult decipi, ergo decipiatur" was already used by Martin Luther and arguably has origins in the first century BC.
[2] I.e. like Kevin Mitnick described in his well-known book.
[3] Based on Demosthenes, 385 – 322 BC.
4 I.e., "bellum omnium contra omnes", *Leviathan*, Part 1, Chapter 13, 165; also: *De Cive, Praefatio*, Section 14.
[5] "Si vis pacem, para bellum", of unknown origin.
[6] "Extremes meet", Jean de la Bruyère.
[7] "Silent leges inter arma" and "summum jus summa injuria", Cicero, *Pro Tito Annio Milone ad iudicem oratio*.
[8] Even the often cited *categorical imperative* of Immanuel Kant is of little value for empirical evaluations. Nicolai Hartmann states that: "As long as it claims that all actions should at the same time hold up as general laws, it is obviously in conflict with each individual's interests. In contrary everybody must want to have something in his own actions which *differs* from the behaviour of everybody else, and which he is the only one allowed to do. Without this, there are no individuals but only replaceable entities within a mass of humans – existence is futile and worthless.", [translated by the authors]. The same claims have been made in publications by the UN and OECD, e.g., the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html,

multicultural, multi-perspectivity and multiple identities it is very difficult, if not impossible, to create standardized norms or laws. We think that, in order to build potential ethical guidelines, even theoretical ethical approaches have to be revisited – this is due to the fact that in the context of IT security ethical concepts are prone to self-awareness problems. A reassessment of the respective value, i.e., a change of perspective and a revaluation of values, is necessary in order to reach new borders, break the circle of self-reference and reduce the amount of black-and-white attitudes. Again, we would like to point out that pure ethical discourses lead into a dead end, as they do not provide us with adequate tools.

In the main part of this work we will lead away from the ostensible ethical discussion on hacking and IT security in order to show that the actual topic is not about ethical problems. Rather, these can be resolved to aesthetic questions. With the help of this evaluation we would like to contribute to lasting solutions. We target a constructive discussion about liability attribution and broaden the horizon of possible solutions in order to shape the future of ethical standards in the field. The conclusions are based not only on theoretical arguments, but on practical considerations as well.

In general we would like to abstain from the rather complex subject of *ethical responsibility* as it is used in the existing debates. At this point we would like to refer to, e.g., the works of Hans Lenk, who extensively analyzed concrete examples from several areas and discussed the multiple dimensions of individual liability, institutional liability and cooperative liability. Starting from Lenk's point, we would like to take the next step further, which brings us directly in *media res*: we can immediately see that *liability* is always constructive and relative; it is social and idealized, hence stuck with a multitude of different expectations, evaluations and interpretations.

The special point in the area of IT security is, as opposed to other fields of science, its inherent fluent border to morale. It is our task to question her current Janus-face of *good and bad*, which does not only appear in the context of sporadic and a posteriori attempts to determine liability.[9]

2 Social-Psychological Approach: Pragmatic Hacking

The most distinctive property of *IT security*, compared to other disciplines, is *security*, i.e., defense against threats. The difference of IT security as compared even to other security disciplines is that the enemy is automated, fast and invisible to the human eye. We would like to emphasize that next to all, possibly even all, security problems exist only because of conflicting human interests. I.e., in the absence of attackers it would be possible to use IT without any kind of security means.

Hence, the threat to defend against is based on human intelligence. Therefore, in addition to strategical and analytical thinking, unconditional properties for IT security specialists are the capabilities of *anticipation*, *empathy*, *flexibility*, *adaptability* and a good amount of *creativity*. However, these properties do not only help the defender, who still might hold back some of his potential in order to keep his system running[10], but also the attacker of a system. It should be noted that both, defensive and aggressive, behaviour can be a possible answer to the same action. Suitability lies within the scope of discretion.

It is interesting to note how Jochen-Thomas Werner characterizes the ideal staff for the executive force, e.g., the police. He emphasises the need to minimize social risks – in an article on homeland security, written for the German police:

> "Four things [...] can be the doom of an acting human: (a) the attitude to be lieve every thing which is printed black-on-white, (b) rigid adherence to, and unreflected believe in, unreasonable pieces of knowledge, (c) the believe to have to act rational while on duty, (d) the perception that a single cause will always result into the same effect."

He motivates this with an "ever created reality" (p. 7) and "there is no single world inhabited by all men. [...]

"UNO Guidelines Concerning Computerized Personal Data Files"
http://www.legislationline.org/documents/action/popup/id/6723.

[9] E.g., comparisons can be drawn also to chemistry where heavy accidents can happen and have happened.

[10] This can be compared to driving a car, where thoughtful driving includes occasional waiving of rights in favour of an increased level of over-all security.

we all live in different socio-cultural universes."

The same conclusion was found by José Ortega y Gasset, while answering the question "What is technology": "Every human is a program, hence he is not what he is, but rather what he wishes to be. (p. 51) [...] In short, humans are terribly different, in contrast to what has been said in the past and by some people of today.". Ignoring this finding will lead, according to him, necessarily to a revolution of the masses.[11] The core message to be found is that the human, and that is: every single individual human, is his own yardstick.

IT Security, and also the activity of hacking, significantly bases on the human aspect in technology – something that has been declined for a long time by rationalists and enlightenment. This is not only demonstrated by the most powerful hacking technique of *social engineering*, but also by the fact that successful attacks on IT systems always base on human imperfection at the most basic level. Even more, this is only the tip of an iceberg of the general tendency in technology to mode more towards social areas. The unique situation of IT security issues is the combination of two extremes: namely complex technological problems, combined with (irrational, abysmal) human interaction. This justifies a special position of the science "IT security". The technical complexity is one basic reason for a number of security problems, i.e., without the complexity of today's computer systems there would be no security issues.[12] Social relevance of security, e.g., defense against threats, is guaranteed due its multiple facets; or: anthropological research on technological issues can be defensive, as well as offensive. The unique feature is, hence, openness in the preconditions and boundary conditions.

2.1 Ingenious Hacking

In the area beyond ethics we can find answers within *aesthetics* and *art*. It should be noted that in this case we do not consider computer generated art like fractals, ASCII art, and similar, but rather the structure of informatics itself, esp. the *art of IT security*. On this abstract plane we finally recognize that any non-trivial action within the area of IT security and also the area of hacking, is well beyond the definition of "good' and "evil".

When the curriculum of informatics was originally designed, e.g., by Friedrich L. Bauer[13], it was called a "engineering-like humanity science (or human engineering science, if that suits better)" [Bau74]. However, what does that mean in our case? IT is an applied science which creates items, hence it is an engineering science. These items, on the other hand, are without doubt immaterial – this can best be seen in liability questions.[14] Still, there is a big difference between natural sciences and IT security: the task of natural science is to find hidden rules, e.g., physical laws or mathematical proofs – and scientific progress is strictly moving along (or around) these lines. It is impossible in natural sciences to invent new rules contradicting physical laws. On the other hand, there are multiple ways of solving problems in IT security, all of which can be correct and wrong at the same time. We thus see that mathematics and natural sciences have an utopian character, whereas IT security, similar to the fields of humanities, have procedural character. It is best compared to philosophy, which is an open discipline by principle with regard to the basic positions and her potential to develop solutions.

More similarities can be found between IT security and philosophy in the process of working on any non-trivial piece of software:

– there is no meaningful way to quantify the quality of software. In general there are no non-trivial measures at all.
– any subjective feeling of control during the development process is illusory.
– software is never ready.
– the intention of software developers are often misinterpreted by consumers, leading to misappropriate use of the software.

[11] See his other book "*The revolution of the masses*".
[12] Recently, the first operating system kernel has been proven correct. The effort included 30 man years of work for 7,500 lines of code. See, e.g., http://www.theengineer.co.uk/Articles/312631/Safer+software.htm.
[13] One of the co-founders of ALGOL, born 1929.
[14] Liability in general is solved unique in IT, as can be seen in next to all EULAs (End-User-License-Agreements): the developers can under no circumstances be held liable for anything. No other industry can waive liability in a similar way.

In all of these above points the term "software" could be replaced with "philosophical discourse" without loosing correctness. This underlines the link between IT(-security) and the humanities. After all, humans can be considered complex, self-modifying ("open") programs. A momentum of uncertainty, humanities always had to deal with.

Taking these characteristics into consideration, we can take IT security and hacking out of their current state and re-fit them into a new position. If IT is neither a real engineering science, nor a natural science, nor humanities, may be it is closest to *art* – consequently, the same degrees of freedom would apply. Art in general is an area where the accomplishments outreach themselves in multiple aspects. In the case of IT security and hacking manifold borders are crossed; which actually is a necessary pre-condition for their work. We also claim that crossing borders, which implies that the person crossing the border also knows where the border has been, actually *sharpens* the awareness of the borders' presence. Much like a martial artist is not only skilled in injuring people, but also very much aware of a body's weaknesses and hence aware of limiting the use of certain aggressive techniques to appropriate situations.

Art and IT work explorative and multi-dimensional.[15] Art is allowed to provoke and humiliate public morality without having to justify its actions; even more, art is expected to provoke. In order to generate new perceptions hackers have to "provoke", i.e., reassess values and work from different perspectives. The search for questions, answers and gaps[16] is a constitutive characteristic. Especially important are *freedom* and *creativity* in the process of making. Whereas it now becomes clear why ethical discussions make no sense in the area of computer security, as long as they make no sense in art.

The biggest similarity between art and IT are the degrees of freedom compared with other sciences. There is a virtually infinite number of ways of creating systems, the only real distinction and decisions basing on personal style. Esp. in IT and art it is not possible to measure which of two solutions is better, or even: more beautiful. On the other hand, it is common to discuss the beauty of solutions. The presence of personal style hints us to a point beyond ethics and even art, that is: aesthetics.

In order to cope with opposed characters and diverse human thinkings it is inevitable to have the maximum possible freedom and creativity. This is, due to its diversity, no subject of ethical evaluation – it is beyond good and evil, even though it is sometimes morally judged.

On this background it is clear, why war is called the father of all things[17]. This proverb is usually also linked to philosophy, where a discussion has to be preceded by a disagreement in order to take place. The same reasoning applies to IT security, where a conflict of opinions is the actual reason of security breaches. In both cases, i.e. philosophy and IT security, opposites and antagonisms are unconditional pre-requisites for creativity and integrating insights.

3 Conclusion

In the widely known text "The Conscience of a Hacker", also known as "The Hacker's Manifesto" we can see how the discussed dilemma is dissolved – taken that we do not have an ethical but rather an aesthetic problem. On this bases we think that it would be reasonable to extend the legal situation of the IT security industry, and hence also of hacking, into the direction of *art*. Therefore we would like to suggest to pass the *right of freedom of the arts,* called *Kunstfreiheit* in Germanic countries, into law for hackers too.

"The Conscience of a Hacker" is a conscientious working method, which is, possibly at a professional level, directed to the benefit of society. However, at the same time being the devil and the knight of the Data-Highway, respectively the conscience of the (development of) knowledge – as every great insight is Janus-faced.

[15] While philosophy also works in a similar fashion, it primarily does not focus on machines. Natural sciences, on the other hand, are more progressive and linear.
[16] Here: vulnerabilities.
[17] Heraklit, B 53.

REFERENCES

Bauer, F.L., 1974. *Was heißt und was ist Informatik*? In: (ed.) Otte M., *Mathematiker über Mathematik*, Springer, Berlin, p. 357.

Blankenship, L, January 8 1986. *The Conscience of a Hacker*. Originally published at Phrack, Volume One, Issue 7, Phile 3 of 10.

Hartmann, N, 1949, *Ethik*. De Gruyter, Berlin.

Lenk, H., 1999. *Praxisnahes Philosophieren*. Kohlhammer, Stuttgart.

Lenk, H et al., 1991. *Technikverantwortung. Güterabwägung – Risikobewertung – Verhaltenskodizes*. Campus-Verlag, Frankfurt a. M.

Mitnick, K.D. et al., Dec. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. Wiley, Indianapolis.

Ortega y Gasset J., 1949. *Betrachtungen über die Technik*. Deutsche Verlagsanstalt, Stuttgart.

Werner, J.-T., 2002. *Netzwerk innere Sicherheit*. http://www.polizeinewsletter.de/documents/innereSicherheit.pdf

KIT Scientific Working Papers
ISSN 2194-1629

www.kit.edu