On the role of human morality in Information System Security

The problems of descriptivism and non-descriptive foundations

MIKKO T. SIPONEN
University of Oulu, Department of Information Processing Science

Key words: Ethics and information security, Information security management

Abstract: The question of whether ethics and human morality can serve as a means of protection against information system security breaches has been brought up recently. The existing views concerning the role of ethics in information systems security can be divided into two categories. These are 1) expressions about the use of human morality and 2) arguments claiming that the use of ethics is useless or very restricted. However, the former views are too general statements lacking concrete guidance and the latter viewpoint is based on cultural relativism, and can be thus classified as descriptivism. This paper argues that descriptivism (e.g. doctrine of cultural relativism) leads to several problems such as *reduction ad absurdum* and it is hence more problematic than non-descriptivism. Therefore, we propose an alternative approach to using ethics in minimising security breaches that is based on non-descriptive theories. The limitations of non-descriptivism (and appealing to human morality in a general sense) will also be discussed. The use of non-descriptivism will be demonstrated using Rawls' concept of the "veil of ignorance."

1. INTRODUCTION

With a technology that is aimed at being used by people, the role of the user is important: ultimately it is the user who determines how effectively the technology is used. This is also true in the case of information systems security, where the efficiency of security solutions and other procedures depend a great deal on the ability and motivation of the end users to comply with provided security solutions/procedures. Many studies indicate that the

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

users' desire to comply with information security guidelines is often passionless (e.g. Parker, 1998; Perry, 1985; Goodhue & Straub, 1989), which, if true, is a weakness with regard to organizational security. To tackle such a weakness, several proposals have been made, ranging from 1) increasing the users' motivation (e.g. McLean, 1992; Perry, 1985; Siponen, 2000a); 2) using ethics (e.g. Kowalski, 1990; Leiwo & Heikkuri, 1998a,b); 3) organizational/professional codes of ethics (e.g. Harrington, 1996; Straub & Widom, 1984; Parker, 1998), 4) to using different deterrents (Straub, 1990). This paper concentrates on the second issue, namely, whether ethics can function as a means of protection in terms of security. This possibility, induced by human conduct, has been recognized by several authors, including Kowalski (1990), Baskerville (1995) and Siponen (2000a).

> "*Security administrators are realizing that ethics can function as the common language for all different groups within the computer community*" (Kowalski, 1990).

> "*Proper user conduct can effectively prevent* [security] *violations*" (Baskerville, 1995 p. 246).

Unfortunately, these proposals do not suggest any concrete means for using ethics in that respect. Consequently, a concrete guidance of how ethics can be used as a means of protection is still needed. The aim of this paper is to propose a framework for the use of ethics in that respect. To achieve this goal, a powerful critique against usability of ethics (and its restrictions) should be considered: the possibility offered by human morality has been criticized by Leiwo & Heikkuri (1998a,b) on the grounds of cultural relativism. If cultural relativism is valid as an ethical doctrine, the use of human morality as a means of protection is very questionable. It could only be possible in certain "security" cultures - i.e. cultures among which security norms have been established - if at all. However, the objection of Leiwo & Heikkuri (1998a,b) is argued to be questionable since A) its foundations build on cultural relativism generally and B) their application of Hegel's doctrine leads to several contradictions.

This paper is organized as follows. In the second section, the objection to use of ethics as a means of protection is considered and in the third section, an alternative approach based on non-descriptivism is suggested.

2. PROBLEMS OF NON-DESCRIPTIVISM

According to Leiwo & Heikkuri (1998a,b), Kowalski's claim (ethics could serve as a protection mechanism against security violations) is not

possible in a large or global environment (e.g. the Internet), on the basis of cultural relativism. They argue that moral values are subjective in the sense that they cannot be transferred from one place or moral system to another (Leiwo & Heikkuri, 1998b p. 275). In other words, the morality of an action depends for example on culture or individuals. See (Taylor, 1975; Hare, 1976) for more on relativism. This argument by Leiwo & Heikkuri also involves ethical descriptivism, since they indicate that moral judgement has a truth value (e.g. true/false): "*the truth values of ethical value systems...*" (Leiwo & Heikkuri, 1998b p. 275). To claim that a moral judgement is true or false is a descriptivistic claim - see Hare (1976; 1997) for an overview concerning the terms descriptivism and cognitivism.

They further engage in cognitivism, which is mainly an epistemological claim stating that values can be known to be true. In the case of cultural relativism generally, exploring the moral values of certain cultures validates this cognitivistic claim. And because it is a sociological fact that morality (what people do/consider as right and wrong) depends on culture, a relativist claims that what everyone does is equally right or true. Due to such epistemological inference, the concepts moral relativism, cultural relativism and ethical relativism are often used to refer to the same concept. The reasoning of Leiwo & Heikkuri is similar to this. To indicate that moral views differ in such a manner with respect to information security, and because of that fact cultural relativism is valid, the culture of hackers and hacker ethics was provided as a proof (Leiwo & Heikkuri, 1998b p. 275). The provided hacker ethics, as reasoned by a legendary hacker "Knightmare", seems to imply subjective/psychological egoistic or radical liberalism[1]. Since "hacker ethics" and cultural relativism were given by Leiwo & Heikkuri as an example to indicate the inadequacy of Kowalski's thesis, these need to be considered more thoroughly next.

First, the approach of Leiwo & Heikkuri does not count on factual/normative dualism that is generally considered to be a valid (explicitly an *ad ignorantiam*) thesis. For example, consider Hume's law "no ought from an is" in this regard, which is, sharing the view of Popper, "*perhaps the simplest and most important point in ethics*" (Popper, 1948). "No ought from is" simply means that factual premises, i.e. 'is' matters cannot imply norms, i.e. 'ought' statements. Here Leiwo & Heikkuri

[1] Knightmare: "*This is a set of beliefs that I have about the world of computers. It may not be what you believe, but that's all right. Hacking has to do with independence*" (Fiery, 1994 p. 161). The aforementioned implies subjective egoistic (e.g. as put forth by Hobbes) and/or radical liberalism (when the latter is used as a moral qualifier) type of viewpoints. A thesis such as "*It may not be what you belief, but that's all right. Hacking has to do with independence*" includes a touch of radical liberalism. Moreover, such statements as "independence" and "*hacking is something that I am going to do regardless of how I feel about its morality*" (Fiery, 1994 p. 162) seem to indicate egoism.

(1998a,b) fall into this fallacy by first observing "is" matters. And as "is" matters (herein hacker ethics or hacker ideology) exist, due to relativism (what every culture does is right, as considered earlier), the actions of hackers (herein hacker ethics) are right per se ("ought" - a norm). Of course, although there are attempts to prove the invalidity of Hume's thesis "no ought from an is" including Searle (1964); Gewirth (1974) and MacIntyre (1981), they do not serve as persuasive objections especially in favour of cultural relativism. For example, Searle's attempt to break Hume's law is widely criticised being a game a promising game, which can only be played if the players accept the rules of game provided by Searle (Hare, 1964). It may only serve as an indication that it may be possible to persuade someone to form an "ought" (e.g. moral) judgement by giving "is" matters without "ought" matters. But does this prove that kind of treatment would be desirable? The most difficult problem into which Searle is falling, is that "the rules of this game" are based on persuasion without any restrictions regarding the contents of the strategy agreed upon, which means that the game is for instance open to lying. Hence, it could be objected that if lying is accepted, we are throwing ethics and morals out of the window. For another example, Gewirth's idea (of equality) is closely connected to the universality thesis, which serves as a basis for his ethical theory/socio-political theory (e.g. see Gewirth 1978), and therefore, even if accepted, may not help cultural relativists.

The weakness behind the thesis of Leiwo and Heikkuri (1998a,b) can also be considered by giving a more down-to-earth example. To see the weakness, consider the following separation. It is a quite a different matter to argue 1) that people's moral conception reflects a certain value conception common to groups of persons, communities, cultures 2) than to accept (in the view of a cultural relativist) that, what a group of people, culture and so on does is right per se, and thus outsiders should not interfere with it. The latter view (2) is difficult to share as it includes a source of difficulties that shall be considered here. Consider the following caricature example that shows the weakness of relativism. An employee is working in a company (the employee is involved in a top secret project). Presume that the employee has joined a gang that has its own moral code and assume that the company have accepted their employee's joining the gang and its culture (the company considers the activities of the gang as harmless). Later, the gang starts to take an interest in philosophy and find out that their background is rather different and somehow it has been forgotten. As they are in favour of cultural relativism they do a kind of "who are we really/what are our moral values" perusal (e.g. provided by Sandel, 1982). It is a way to reflect "is" matters, i.e. how things were/are, and to allow this to determine how things should ultimately be/how we ought to act. As a result of this, they find a new

moral code that better reflects their original background. They are also positive that this is their real moral code, which was simply not noticed until now. This code includes hacking - result being that the employee should break into his company's system (or otherwise allow the gang to access top secret information). If the company and the employee acknowledge cultural relativism as a valid moral qualifier, they have no (moral) right to either prevent such actions or take any stand with respect to these actions, otherwise they have interfered with the "other culture". Thus as mentioned, any (moral) involvement with the other culture is not acceptable according to cultural relativism, as moral values are subjective. Therefore, the company in our example cannot take any moral stand concerning some other culture (the gang in our example). Some of us may find such treatment very counter-intuitive.

To continue with practical consideration about hacker ethics, consider Knightmare's argument for it: "*hacking is something that I am going to do regardless of how I feel about its morality*" (Fiery, 1994 p. 162). It is difficult to see how such an unconcerned view with respect to morality can have any kind of juncture with the domain of moral discourse (or real 'hacker ethics' if you prefer). However, these kinds of stances to side-step moral reflection outright (as Knightmare is likely to do) can be justified given that cultural relativism is interpreted as a valid moral qualifier. That is to say that Knightmare could insist that the hackers such as Knightmare, for instance, form a culture and due to cultural relativism, we should allow them to do whatever they do. This line of reasoning can seriously flawed with respect to moral life, at least given that we see important to truly attempt to find what is right and wrong, not avoid it nor uphold dogmatism as is likely to be (consider "*regardless of how I feel about its morality*" that is likely to imply dogmatism towards hacking) the case with Knightmare.

Moreover, a totally relativistic view is not shared by Hegel either, who Leiwo & Heikkuri (1998a,b) use to back up their claims concerning the validity of relativism and hacker ethics. Although Hegel views that "*What is both must and ought to be*" (Sabine, 1963 p. 627) he seems to recognise a problem related to standard cultural relativism. Namely, in epistemological sense, standard cultural relativism implies that all beliefs/belief systems are equally true. In Hegel's account however, any possible conflicts should be organised ensuring one's freedom (understood as a social phenomena, a property of the social system in question that rises through moral development of the community) and above of all the coherence of state (i.e. government/country) (Sabine, 1963 p. 655). Hence, anyone following Hegel's scheme must explore, for example in the case of conflicts between advocates and non-advocates of hacking, which alternative ensures the coherence of state. This is interesting, since hacker ethics contains a rule

"*mistrust authority - promote decentralization*" that, if applied, is likely to imply that governments should be mistrusted as well. Therefore, hacker ethics is likely to be in conflict with Hegel's idea. Recall that in Hegels' account, we should ensure the coherence of the state and it is difficult to view "mistrusting authority" as maintaining the coherence of the state. The same is likely to be true with a norm of hacker ethics: "*all information should be free*", which may also not maintain the coherence of state, and is therefore wrong from the Hegelian viewpoint. If the aforementioned reasoning is correct, arguments based on Hegel and "hacker ethics" as provided by Leiwo & Heikkuri (1998a,b) seem to have a source of conflict.

It also seems to be rather illogical to build on the theory of cultural relativism (explicitly the reduction *ad absurdum* type of problem), as it does not make any logical sense to claim that all moral judgements are relative while maintaining that moral relativism itself is absolutely true (being non-relative). If all moral beliefs are relative, as relativists may claim, absolutely true theories are an impossibility (Hare, 1986; Niiniluoto, 1990). This would also apply to cultural relativism.

The contribution of Leiwo & Heikkuri (1998a,b), however, serves to point out a possible problem related to moral discourse. There may be difficulties to share certain common moral notions, especially in a pluralistic value environment such as the Internet. But, neither these difficulties nor cultural relativism do necessarily imply that there cannot be critical moral discussion between different moral beliefs concerning what is right and wrong or how things should be?

3. NON-DESCRIPTIVISTIC USE OF ETHICS

The central task of moral philosophy is to determine what kinds of actions are right or wrong (Warburton, 1996; Hare, 1981). Cultural relativism fails to accomplish this mission: it does not explore what is ultimately right or wrong, but emphasizes what is right or wrong in certain cultures. We see that non-descriptivism better satisfies the task of moral philosophy and the requirements of human morality: it endeavors to justify the principles of the moral enquiry and then uses them. In that light, it is clear that moral philosophy would be truly useful for security only given that the security actions themselves are morally right. It should be noted that security actions *per se* might not always be morally right. This is so because the aims of information security can be depicted for example by using the requirements of confidentiality, integrity and availability, etc (while moral philosophy search what is right action). As a corollary, security is not ethics

(or vice versa), and security activities are not automatically ethically/morally right.

However, as almost any activity can also be viewed from an ethical point of view, it may be seen that information security relates to the ethical dimension in a special way. Information security protects against actions that often raise concerns regarding morally right or wrong actions (whether or not these views are dogmatic beliefs or all-things-considered beliefs, i.e. beliefs reasoned with thorough moral scrutiny). Although people are commonly argued to be moral beings, and as a result, avoidance of moral reflection is seen as almost impossible (Taylor, 1975; Warburton, 1996), people are often reported to be incapable of extending their thinking to cases where IT is involved (e.g. Severson, 1997). This is due to various reasons, such as unawareness, moral distance or conventional moral notion.

Unawareness (I) and conventional moral notion (II) may be overcome, for instance, when one's moral sense is "awakened" (perhaps a possible cure for I) and moral philosophy can be used to discover what is right and what is wrong (insofar as it can be revealed by moral philosophy) and find justness (perhaps a possible cure for II). This kind of use of ethics to reveal what is right/wrong can be positive or negative from the perspective of information system security. The former (positive) might be the case, for example, when the activities of an organisation can be proved to stand up to moral perusal and most of security violations occur due to clearly unfair activities by persons who are unaware of the real nature of their actions that cannot stand up to moral perusal. However, this may not always be the case. Moreover, ethics can be used to appeal to behaviour in the sense of indoctrination having perhaps both positive and negative consequences from an organisational point of view; perhaps positive for a short period and most likely negative in the long run. The negative state of affairs (II) from an organisational point of view may be the case, at least for a short period, when organisational activity cannot stand up to closer moral inspection. However, this situation may give positive results in the long run, if this kind of scrutiny nullifies the double standard of morality and creates a trust between employees and employer that can stand up to moral scrutiny. Acting in accordance with moral responsibility is likely to be much more "motivating" than acting against it (e.g. Hare, 1981). The following guidelines for using ethics to persuade the listener can be used:

- Justify the principles (e.g.' veil of ignorance'/universality principle as below): state that the chosen principle is the best possible in the situation.
- Apply this principle (and justify the claim that the situation is morally acceptable).

3.1 An example of use the 'veil of ignorance'

Let's take a traditional simple example in which people are considering whether hacking is allowed, i.e. whether is it morally acceptable to obtain access into information systems. We shall consider this action in the light of simplified version of Rawls' theory of justice, which is affiliated with the universality principle proposed by Kant, Hare (1981), Christian ethics (The Golden Rule) and Gewirth (1978). The limitations of the 'veil of ignorance' are discussed in Kukathas & Pettit (1990), and the limits of universality principles are discussed generally in Siponen (2000b). The concept of 'veil of ignorance' has a key role of Rawls' theory. He proposes that the principles of justice should be selected in an imagined 'veil of ignorance.' Under the veil of ignorance we are ignorant of our status, age, gender and the like. In doing this, the veil of ignorance strives to achieve impartiality since we are choosing principles that are equal for all, irrespective of our differences in terms of age, status, gender, etc. These qualifiers are ruled out since there are likely to be morally irrelevant to the choice of principles of justice (Rawls, 1972; Hare, 1963; 1981; 1989; Siponen, 2000b). So, in the case of hacking, given that application of the veil of ignorance desired, we need to imagine a situation in which we are unaware of our social status, age, sex, profession, etc. From behind of this veil of ignorance we would need to ask ourselves whether we accept that hacking would be allowed for everyone -- so, anyone and everyone could break into our systems at any time. We submit that most of us, under the veil of ignorance, would not accept hacking.

4. CONCLUSIONS

This paper has analysed the role of ethics as a means of protection against security breaches. An attempt to show that ethics cannot serve as a protection mechanism in a global environment with the help of cultural relativism was considered. It was pointed out that such a claim does not count on normative/factual dualism, since it violates Hume's law "no ought from an is". Another logical weakness of this thesis, *reduction ad absurdum*, was shown: to claim that all beliefs are relative is self-refuting. Moreover, it was shown that cultural relativism could lead to dogmatism, for example blind belief in hacker ethics.

We endeavored to justify and show a non-descriptive way that ethics can be used as a means of protection. This idea simply reflects the main objective of ethics: to answer moral concerns, i.e. discern what is morally right and wrong and to use ethical discussion that is often persuasive by

nature. A two-step guideline in this respect were put forth: to chose and justify the theory and apply it. It should be noted that the use of ethics is not a panacea. There is evil in the world (e.g. Warburton, 1996). This means that there are likely to be people who want to behave egoistically or maliciously, regardless of the moral status of that behavior.

5. ACKNOWLEDGEMENTS

I am grateful to Mr. Pekka Abrahamsson, Prof. Juhani Iivari and Docent Kari Väyrynen in the University of Oulu, Finland and Dr. Jussipekka Leiwo at the Division of Mathematics and Computer Science in the Amsterdam Free University, for their comments on the earlier version of this paper. I would also like to thank the anonymous reviewers of the 15th International Conference on Information Security, for their comments.

6. REFERENCES

Baskerville, R., (1995), The Second-Order Security Dilemma. in W. Orlikowski, G. Walsham, M. Jones and J. DeGross (Eds.) Information Technology and Changes in Organizational Work. London: Chapman & Hall, pp. 239-249.

Fiery, D., (1994), Secrets of a Super Hacker. Loompanics Unlimited, Port Townsend, Washington, USA.

Gewirth, A., (1974), The 'Is/Ought' Problem resolved. Proceedings and Addresses of the APA 47 (1973-74): 34-61.

Gewirth, A., (1978), Reason and Morality. The University of Chicago Press, USA.

Goodhue, D.L., & Straub, D.W., (1989), Security Concerns of System Users: A proposed Study of User Perceptions of the Adequacy of Security Measures. Proceedings of the 21nd Hawaii International Conference on System Science (HICSS).

Hare, R. M. (1963), Freedom and Reason. Oxford University Press.

Hare, R.M., (1964), The Promising Game. Revue Internationale de philosophie 70.

Hare, R.M., (1976), Some Confusions about Subjectivity. In Freedom and Morality (eds.): J. Bricke. Kansas University Press.

Hare, R. M., (1981), Moral Thinking: its levels, methods and point. Oxford University Press, UK.

Hare, R.M., (1986), A Reductio ad Absurdum of Descriptivism. Philosophy in Britan Today. edited by S. Shanker. Croom Helm, London, UK.

Hare, R.M., (1989), Principles. In R. M. Hare (eds.): Essays in Ethical Theory, pp. 48-65. Oxford University Press, UK.

Hare, (1997), A Taxonomy of Ethical Theories. In R.M. Hare (eds): Sorting out Ethics. Oxford University Press, UK.

Harrington, S. J., (1996), The effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgements and Intentions. MIS Quartely, Vol. 20, No. 3, September.

Kowalski, S., (1990), Computer Ethics and Computer abuse: A Longitudinal Study of Swedish University Students. IFIP TC11 6th International Conference on Information Systems Security.

Kukathas, C. & Pettit, P., (1990), Rawls - A Theory of Justice and its Critics. Stanford University Press, California, USA.

Leiwo, J. & Heikkuri, S., (1998a), An Analysis of Ethics as Foundation of Information Security in Distributed Systems. Proceedings of the 31st Hawaiian International Conference on System Sciences (HICSS-31).

Leiwo, J. & Heikkuri, S., (1998b), A Group-Enhanced ISSI Model for Secure Interconnection of Information Systems. Proceedings of the IFIP TC11, 14th International Conference on Information Security (IFIP/Sec'98).

MacIntyre, A., (1981), After virtue. A Study in Moral Theory. London, UK.

McLean, K., (1992), Information Security Awareness - Selling the Cause. Proceedings of the IFIP TC11 (Sec'92).

Niiniluoto, I., (1991), What's wrong with relativism. Science Studies, Vol. 4, No. 2, pp. 17-24.

Parker, D. B., (1998), Fighting Computer Crime - A New Framework for Protecting Information. Wiley Computer Publishing. USA.

Perry, W.E., (1985), Management Strategies for Computer Security. Butterworth Publisher, Boston, USA.

Popper, K., (1948), What can Logic do for Philosophy? Aristotelian Society, Supplementary Vol. XXII.

Rawls, J. A., (1972), A Theory of Justice, Oxford University Press, UK.

Sabine, G.H., (1963), A history of Political Theory. Third edition. London, UK.

Sandel, M., (1982), Liberalism and the Limits of Justice. Cambridge University Press, UK.

Searle, J., (1964), How to Derive "ought" from "Is". Ph. Rev., 73.

Severson, R. J., (1997), The Principles of Information Ethics. Armonk (N.Y.) M. E. Sharpe cop. USA.

Siponen, M.T., (2000a), A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security. Volume 8, Issue 1, pp. 31-41.

Siponen, M.T., (2000b), The Relevance of Software rights: An Anthology of the Divergence of Sociopolitical Doctrines. AI & Society. Furthercoming.

Straub, D. W., & Widom, C. P., (1984), Deviancy by Bits and Bytes. In Computer Security: A global challenge, J.H. Finch and E.G. Dougall (eds.): Proceedings of the Second IFIP International Conference on Computer Security (IFIP/Sec'84).

Straub, D. W., (1990), Effective IS Security: An empirical Study. Information System Research. Vol. 1, Number 2, June, p. 255- 277.

Straub, D. W. & Nance, W. D., (1990), Discovering and Disciplining Computer Abuse in Organization: A Field Study. MIS Quartely. Vol. 14, No. 1, March.

Taylor, P.W., (1975), Principles of Ethics - An Introduction. Dickenson publishing company. Encino, California, USA

Warburton, N., (1996), Philosophy: the Basics. Second Edition. T J Press Ltd Padstow, Cornwall. UK.