Vulnerabilities as monsters: the cultural foundations of computer security (extended abstract) [⋆]

Wolter Pieters and Luca Consoli

Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
{w.pieters,l.consoli}@science.ru.nl

Abstract. This paper is part of a project to investigate the philosophical aspects of the scientific discipline of information security. This field of research investigates the means to protect information systems against attacks, typically by modelling the system according to a certain security model, and verifying the conformance. In this contribution, we study the relation between models of information security, and cultural categories that help us to describe the world. According to Martijntje Smits, cultural categories necessarily produce phenomena that do not fit in the categorisation. From a negative perspective, these phenomena can be characterised as monsters: they have properties of two categories that were thought to be mutually exclusive, like many monsters that appear in films. Smits applies this anthropological approach to explain controversies around the introduction of new technologies in our society, such as the current debate on genetically manipulated food. We translate this framework to the scientific enterprise of information security, by explicating the analogy between Smits's monsters in society and system vulnerabilities in information security. We argue that several important security threats, such as viruses in Word documents, have been produced by phenomena that did not fit into existing cultural categories of computer science, in this case the categories of programs and data. Therefore, they were not included in security models. Based on our analysis, we describe the cultural foundations of information security research, we search for strategies for dealing with vulnerabilities-as-monsters analogous to Smits's strategies for dealing with monsters in society, and we discuss the consequences of our approach for responsibilities of computer scientists.

Information security can be defined as the scientific discipline that deals with protecting information systems against attacks. Research typically concerns (formal) methods to avoid or eliminate security vulnerabilities in information system design. However, information security also has a social side, typically discussed in terms of trust in information systems. Unfortunately, the implicit philosophy behind the research covering this social side is rather naïve. It assumes a distinction between "actual security" and "perceived security": scientists describe actual security, and public trust is based on

[⋆] This work is supported by a Pionier grant from NWO, the Netherlands Organisation for Scientific Research.

perceived security [2, 9, 10, 12, 16]. Explicit philosophical work on information security is rare.[1]

In a previous paper [11], we argued that the sketched implicit philosophy of information security, based on the distinction of actual and perceived security, is problematic from a philosophical perspective, and we provided two general arguments for this thesis. The first is the results of Science and Technology Studies (STS), which have shown that scientific facts are not directly linked to "actual" reality, but rather constructed in a process of interaction and negotiation ([6], p. 7). The second is the inherent fallibility of security assessment: one never knows what attackers will be up to in the future. It is the latter argument that we will focus on in the current study. This paper is therefore part of a project to investigate the philosophical aspects of the scientific discipline of information security.

We think that the inherent fallibility of security assessment can be explained in terms of cultural categories, and phenomena that do not fit into these categories. Cultural categories are classifications that help us describe and understand the world. In her PhD thesis, Martijntje Smits ([15], see also [14]) argues that controversies surrounding the introduction of new technologies can often be explained in terms of a clash between cultural categories. For example, we may think of genetically manipulated food as an (unacceptable?) mixture of nature and culture. Classification problems are deeply entrenched in human culture. Some African tribes considered twins as monsters, because, according to their categories, only animals produced more than one child, and twins thus had both human and animal traits. These "monsters" come into being when cultural categories are inadequate to fit phenomena.

Smits argues ([15], p. 143, our translation): "From the monster theory it follows that waste and dangers are inevitable, because they are the unintended by-products of cultural category classifications. On the borders of these classifications, ambiguities appear, that may, among other things, manifest themselves as monsters." The latter happens when the ambiguity is experienced negatively, and cannot be resolved easily. The term "monster" can be understood by reference to monsters in stories and films, which often combine elements of different categories as well.

We see a strong analogy here with the fallibility of security assessment in computer science. The most spectacular attacks on computer systems often occur when this way of attacking has not been considered before. In other words, when the vulnerability does not fit into the existing *categories* of computer security. As much as society will always produce waste and dangers because of existing categories, computer security will always produce vulnerabilities because of existing security models. Categories used in scientific analysis are seen as cultural categories here as well.

A typical example of a clash of categories in computer security was the issue of viruses in Microsoft Word documents [5, 4]. Up till a certain point in time, viruses were supposed to hide in executable files (i.e. programs) only, not in documents. The viruses in Word documents were a clever example of the mixing of two cultural categories in computer science: those of programs and data. An interesting question is who was responsible for this clash. Was it Microsoft, who allowed macros to be executed in

[1] There is some general work on philosophy of information systems that could be applied to information security, e.g. [3, 1]. However, we will take a different approach in this paper.

Word documents? Was it the virus writer, who exploited this feature in order to attack systems? Or was it the computer science community, whose classifications were not suitable for all types of files?

Following the monster theory, any classification in computer science that affects or models security is bound to create vulnerabilities as by-products. The conceptual separation of programs and data produced the text document viruses. The separation of the hardware level and the software level in smartcards produced the power analysis attack, in which data could be read by eavesdropping on the power consumption of the card [8]. Of course, from a legal perspective, the attackers are responsible for the problems involved. But on a more fundamental level, the cultural categories themselves are responsible for providing the opportunities for attack. Such vulnerabilities can be understood as monsters, and this provides one of the ingredients for a more subtle philosophy of information security.

Smits considers four different ways of dealing with monsters: embracing, expelling, adapting, and assimilating. Can they be used for dealing with vulnerabilities in computer security as well? Embracing the monster as a wonder may happen among hackers, but a vulnerability is generally not perceived as such within the computer security community. Expelling the monster is not feasible, because a threat to a computer system cannot be eliminated as easily as a new phenomenon in society, since the attacker is typically outside the control of the computer security community. Still, it might help to say “there is no problem” and see if everything stays quiet. Adapting the monster may be useful, for example by categorising Word documents as executable files rather than data files, which is done in virus scanners today. In such an approach, the threat becomes one of a known category: a virus in an executable file. However, this presupposes a unidirectional relation between categories and the phenomena they explain, which does not do justice to the complex interaction in which categories are formed.

The last strategy Smits mentions is assimilating the monster, a process in which both the monster and the cultural categories are being changed. Thus, power analysis attacks now have their own field of research, and the vulnerability has changed from a side-effect to something that can actually be prevented using appropriate tools. This means that both the categories and the technology have been changed, by assimilating the monster of power analysis attacks. From an ethical point of view, the possibility of assimilating monsters leads to new kinds of responsibilities. Members of the computer security community are not only responsible for formalising all aspects of existing categories, but rather for contributing to the evolution of the categories themselves, so that they are better able to incorporate new phenomena, and thereby prevent new attacks.

Smits argues that assimilating is the best style of dealing with monsters, and we may agree from a computer security perspective. For there is no final model of information security that incorporates all vulnerabilities, as there is no final set of cultural categories that fits all phenomena.

References

1. P.J. Dobson. The philosophy of critical realism – an opportunity for information systems research. *Information System Frontiers*, 3(2):199–210, 2001.

2. D. Evans and N. Paul. Election security: perception and reality. *IEEE Security & Privacy*, 2(1):24–31, January/February 2004.
3. L. Floridi. Information ethics: on the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1(1):37–56, 1999.
4. R. Ford. Why viruses are and always will be a problem. *NCSA News*, pages 5–7, April 1996.
5. S. Gordon and R. Ford. Real-world anti-virus product reviews and evaluation. In *Proceedings of Security on the I-WAY*, Crystal City, Virginia, 1995. NCSA.
6. J. Keulartz, M. Korthals, M. Schermer, and T. Swierstra. Ethics in a technological culture: A proposal for a pragmatist approach. In J. Keulartz, M. Korthals, M. Schermer, and T. Swierstra, editors, *Pragmatist ethics for a technological culture*, chapter 1, pages 3–21. Kluwer Academic Publishers, 2002.
7. H. van Lente. *Promising technology. The dynamics of expectations in technological developments*. PhD thesis, Univ. of Twente, Enschede, 1993.
8. T.S. Messerges, E.A. Dabbish, and R.H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5):541–552, May 2002.
9. P. Nikander and K. Karvonen. Users and trust in cyberspace. In B. Christianson, B. Crispo, J.A. Malcolm, and M. Roe, editors, *Security Protocols: 8th International Workshop, Cambridge, UK, April 3-5, 2000, Revised Papers*, number 2133 in Lecture Notes in Computer Science, pages 24–35. Springer, 2001.
10. A.M. Oostveen and P. Van den Besselaar. Security as belief: user's perceptions on the security of electronic voting systems. In A. Prosser and R. Krimmer, editors, *Electronic Voting in Europe: Technology, Law, Politics and Society*, volume P-47 of *Lecture Notes in Informatics*, pages 73–82. Gesellschaft für Informatik, Bonn, 2004.
11. W. Pieters. Acceptance of voting technology: between confidence and trust. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management: 4th International Conference (iTrust 2006), Proceedings*, number 3986 in Lecture Notes in Computer Science. Springer, 2006.
12. R. Riedl. Rethinking trust and confidence in european e-government: Linking the public sector with post-modern society. In *Proceedings of the Fourth IFIP Conference on e-Commerce, e-Business, and e-Government (I3E)*, 2004.
13. B. Shneiderman. Designing trust into online experiences. *Communications of the ACM*, 43(12):57–59, 2000.
14. M. Smits. Monster ethics: a pragmatist approach to risk controversies on new technology. In *Proceedings of the Research in Ethics and Engineering conference*. Technical University of Delft, April 25–27 2002.
15. M. Smits. *Monsterbezwering: de culturele domesticatie van nieuwe technologie*. Boom, Amsterdam, 2002.
16. A. Xenakis and A. Macintosh. Procedural security and social acceptance in e-voting. In *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05)*, 2005.