A Case Study in Malware Research Ethics Education

When teaching bad is good

John P Sullins
Department of Philosophy
Sonoma State University
1801 East Cotati Ave.
Rohnert Park, CA 94928
Email: john.sullins@sonoma.edu

***Abstract*—There is a growing interest in the research of malware in the context of cyber-security. In this paper I will present a case study that will outline the curriculum used to teach malware ethics within the context of a computer science course that teaches students malware programing techniques. Issues from computer and information ethics that apply most closely to ethical malware research will be highlighted. The topics discussed in the course will be outlined and assessment techniques will be discussed.**

Keywords—Malware ethics; computer ethics; research ethics; information ethics; malware education

I. INTRODUCTION

Today, there is a growing interest in the research of malware in the context of cyber-security and this has inspired some university courses which are now taught on the subject as well as some interesting collaborations between universities and the industry of cybersecurity [1]. Academic malware research is also in the self-interest of universities who need to develop skilled professionals in their own campus communities that can help them combat the growing threat universities face from malware attacks, because when it comes to malware, ignorance is not bliss [2].

One of the trailblazers in malware education, Professor George Ledin, teaches a unique course at Sonoma State University where the students are taught malware programing techniques where they are encouraged to interact directly with the design of malware programs in order to develop a comprehensive understanding of what goes into the creation and deployment of the malware threats they will face in their professional careers.

I have been the ethical adviser to Professor Ledin's course on malware design for a number of years now. Given the special nature of this course, both he and I agreed that the issues in computer and information ethics that applied most closely to the ethical research in malware programing would need to be highlighted in the course. Malware programing is dangerous knowledge and it cannot be presented in a university setting without serious moral, as well as technical, firewalls in place. In this presentation I will outline some of the topics we discuss with the students who take this course, how the topics in ethics are presented in the class and our rationale for requiring students to keep ethical norms in mind as they do their research projects involving malware design.

II. MALWARE ETHICS

A. Background and research collaboration

While the field of computer ethics began many decades ago, the topic of malware ethics has been slow to emerge. Ethicists, of course, noticed malware and the damaging effects it had on the growth and acceptance of cyberspace and the challenge malware placed on the hope that the internet could be a legitimate locus for communities that could foster ethical behavior amongst its members. But malware was always seen as the enemy, something to be avoided and discouraged. A cyberethicist need not contemplate the specific technologies and design of malware in the same way that a standard ethicist need not contemplate how to commit crimes. They only needed to worry about how to form ethical systems that would discourage those practices. This resulted in a conceptual blind spot that professional computer ethicists have had towards the more complex reality that exists in the relationship of malware with more legitimate computer programing.

Outside of the community of computer ethicists, computer scientists and others began to notice certain ambiguities about malware. While on one hand it is dangerous software that facilitates abuse, fraud, crime and spying—on the other hand, it does so in interesting and sometimes brilliant ways. In 2005 the computer scientist George Ledin in an article published in Communications of the ACM, proclaimed that education in computer security without courses where the students were taught how to design malware, would be like a medical science that tried to invent cures without ever studying any diseases [3]. Ledin argues that it is in the interest of public good that university students majoring in computer science are offered courses on malware design, as these people will be the ones most trained to help combat the growing malware threats [3] [4]. He has run such a course at Sonoma State University for a number of years now but his effort is not always well understood by the media [5][6][7][8], nor is the movement well accepted within computer science education just yet [4].

DOI 10.1109/SPW.2014.46

Another computer scientist who is at the forefront of malware education at the university level is John Aycock. His work is particularly interesting in that he has written about some of the positive things that can be done with malware and his work confounds the notion that all malware is unethical. He and his co-author argued in [9] that sometimes it can even advance the cause of justice when no other means is available, such as when it is used to protest against oppressive regimes. He has even maintained that malware can have a kind of beauty and artistry that could be utilized in novel art projects [10].

B. Ethical problems in the study of malware

Even if we begrudgingly grant that malware can be technically interesting in its design and that there may be the occasional positive use for malware programing techniques, it must be acknowledged that working with malware is not ethically neutral. Even when we are just trying to deconstruct a piece of malicious programming, it requires that we think like the criminal that wrote it in the first place. Since moral thinking and sentiment is a skill that needs to be developed in each individual, if one actively trains themselves to think immorally, then one might lose the ability to make good choices, much like an undercover cop gone bad through her extended contact with the underworld of crime. This requires malware researchers to develop the difficult skill of compartmentalizing their ability to think nefariously so that it does not overtake their ability to reason morally.

Let's now look at the major ethical issues which are commonly encountered in malware research that have to be addressed.

1) Human subjects in malware research.

One of the primary issues is how human subjects are treated in malware research. While some malware research is concentrated solely on the technical issues surrounding the creation and detection of malware and its interactions with specific computer systems, there are occasions where researchers' actions impact the real lives of others, be they the suspected criminal operators of some botnet, or perhaps the victims who may own compromised machines that the researchers gain access to while studying malware in situ.

In these situations there are many ways the actions of the researcher may unfairly affect persons who may be directly or indirectly involved in a malware outbreak. While this is more of a concern for large industry initiatives that are attempting to control and combat malware abuse, it does crop up in academic research as well. When it does, malware research has not developed a good track record on the ethical treatment of persons affected by the research. As we presented at CREDS 2013, the de facto policy in effect for most researchers is the desire to not do additional harm to those persons who might own machines that are part of an illegal botnet that the researchers might have gained control of for a time in order to study it, but to leave them no worse off than they were before the researchers arrived. We criticized that stance last year [11]. It is important for researchers to know that just because something is legal and "IRB-approved'" it does not mean that their research is therefore ethical. This is due to the special fact that we are often dealing with technologies and situations that have not been effectively legislated, or that occur across many jurisdictions, so the law is often not much help. Additionally, IRB boards may not entirely understand the proposed research and will often neglect the fact that informed consent is not obtained given that it would be impossible to obtain before the research began [11][12].

This means that ethicists working with research ethics boards need to know more about the special considerations of using human subjects in malware research [12][13], but more importantly, researchers have to be well trained to make ethical decisions during their research since they will have to make many novel decisions on the fly that may affect real humans who are completely unaware they are even the subjects of the research. Ethics is not something that can be enforced from outside of any study of malware. The research itself has to be ethically motivated and the researchers themselves must have specific ethical commitments. We will discuss how to achieve ethical motivated malware research in section three.

2) Malware and Information Ethics

Since computer technologies change so rapidly, some ethicists have attempted to find more general ethical norms that might apply to any conceivable information technology. Following along with this trend, I have suggested that, broadly speaking, moral values occasionally conflict with the recording, communicating and organizing of digital information and these conflicts are at the heart of most computer ethics concerns [14]. Malware research adds its own special considerations to these three main conflict areas which can be outlined as follows:

a) Information recording: Data collection without the explicit consent of users is ubiquitous in information technologies. This sad state of affairs does not absolve malware researchers from considering the ethics of the type of data and the manner in which it is collected on the users and victims of malware especially when informed consent is impossible, impractical, or even dangerous for the researchers to attempt [12].

b) Information communicating: Academics place a high value on the free communication of their research findings. Since malware research often uncovers sensitive, private, or even dangerous information, the simple reporting of findings in the normal academic manner may pose ethical problems, e.g., should one publish information on exploits that might facilitate future cybercrime or terrorism. On the other hand, academic freedom is a public good and we must not error on the side of self-censorship either [12]. But it is a tricky balance, as we see in the case of [16], where researchers developed their own malware called "Chameleon" which they used to study how it would spread through unsecured WiFi networks but this kind of research is only valuable if it teaches us something new and it is dangerous if it only refines a known hack and makes it easier or cheaper for those with criminal intent. The researchers in this case make no mention of potential ethical impacts or a justification for the research that they did so there is no record of any ethical deliberations they may or may not have done. We can do better in

communicating our values in our own research. Additionally, researchers in malware often work with, or seek funding from, corporations or military institutions that have a vested interest in the results of the research. It is understandable that researchers find the funding attractive, but this could also diminish academic freedom as the communication of data might be more privileged to those funding the research and the long term goals of the funding agency might be at odds with the personal ethics of the researchers themselves. There is also a very serious potential problem noted in [12], where the authors warn that researchers may be forced to communicate the data they have recorded during malware research by law enforcement and governmental agencies, both domestic and foreign, which can draw researchers into situations they find unethical, but to which they are powerless to resist.

c) Information organizing and synthesis: Here I am thinking of automated behavioral analysis techniques where a system might be designed that analyzes the behavior of processes running in a system and flags them either as malware or safe. Given that legitimate and ethical interests might be inadvertently thwarted by these countermeasures, there might be ethical concerns in their use in malware research.

We will now look at how we address these concerns in an actual malware research course.

III. Case Study—a Corse in Malware Ethics

1) Rationale

A class in malware programing has been taught at Sonoma State University for a decade or more as an elective in its undergraduate Computer Science major [5][6]. Early on, its principal instructor, George Ledin, felt that it was imperative that malware research ethics must play an important role in the course. I was brought into the project to help fill that need, the only problem being that malware research ethics was (and still is) not a highly developed field so there was no way to just import some standard modules on ethics into the course and consider it a job well done. My first inclination was to consider the problems in malware ethics to be similar in nature to computer ethics in general with some concerns in human subject testing similar to those found in medical research ethics. These were good places to start but, as I mentioned in section two, computer ethicists had turned their backs on malware early on and medical ethics had grown slowly out of centuries worth of case studies in medical research was very specific to that milieu and hard to adapt to malware research except in very general terms. This required that I rethink my training in ethics to fit the special milieu found in malware research. An additional constraint is that there was a limited amount of time that could be devoted to explicating the theories that the students would need to apply to their research. The following is an outline of what is taught at the time of the writing of this paper.

a) Basic concepts: While it would be ideal if the students came prepared with a general understanding of ethical theory before the course started, this is never the case in reality, except for the rare student who might have taken my course in computer ethics prior to taking this class. Brevity requires us to start with the ACM Code of Ethics [16]. Codes of ethics are fine, but they can only go so far. Research has shown that "…merely having read the [ACM] Code can improve ethical moral judgment in certain situations" [17]. But more has to be said since many of the researchers will be dealing with novel situations and grey areas that are beyond the purview of the ACM code of conduct. This requires we do a brief a review of some of the greatest hits in ethical theory such as utilitarianism, deontology, human rights, and the unified common goods approach as described by James Moor in [18]. Of course each of these ethical systems has well known strengths and weaknesses, so we have to also focus on some other systems as well to patch those conceptual holes. To do this we use concepts from virtue ethics to serve as a more personal ethics which is needed to help guide decisions that lack precedence or adequate time for forethought due to their novelty. And most importantly, researchers need to be made aware of the growing work in information ethics since it has the greatest level of applicability to their work, given its focus on information as an environment where the interests of groups and individuals interact. All of this is directly focused on issues of privacy, the recording, communicating, and synthesizing of information, and digital rights; e.g. copyright, system access rights, the digital divide, etc.

b) Virtues in Security: Of course, what counts as a virtue is somewhat dependent on the culture you are in. In the liberal democracies that most of the readers of this article will come from, security and the openness and transparency of process which is demanded by liberal democracy are often at odds with each other. The malware researcher spends her entire career torn by these opposite demands on her loyalties. The security industry frequently speaks of the three virtues of secure software, ominously referred to with the acronym CIA; confidentiality, integrity, and availability. This concept is presented to the student researchers but also thoroughly critiqued as we have done in [19], where we show that the "firewall" analogy used in building systems compliant with the CIA principles can be misleading, and that these systems are not impervious to insider threats and the challenges of distributed and mobile computing. We can then discuss the ethics of data level security such as personal encryption and the ethical challenges that poses.

c) Ethical Hacks: Researchers are encouraged to think of themselves not as simple passive receptors of ethical thought, but as active agents involved in the creation of new norms of behavior that will be useful and relevant to the future of humanity as it evolves in the information environment. Malware research is best done by a community of researchers who realize their ethical commitments to one another [19]. Hacking the boundaries and potentials of computer systems is not inherently bad. Sometimes it can result in new innovations and modes of thought about systems that were not present before the hack. What matters is the ethical and moral motivation of the hacker herself. This is why we focus so much on the personal motivations and virtues of our researchers. These personal codes of conduct are more

important and decisive than any institutionally produced code. They provide the final ontological friction to prevent certain unfortunate outcomes. It is the individual programmer who decides whether to put on a white or black hat. Therefore we have to provide each researcher with the ethical concepts they need, along with time to think about their own projects and the ethical implications of the work they are doing.

d) Assessments: currently we assess the progress of the researchers in their ability to apply the concepts they have learned first in a low stakes environment thought the use of classroom discussion and reflections and finally in a more high stakes exam process. Recently we have come across the work in [12], where they have researchers add a section on the ethical warrants and rationales that argue for why the researcher(s) chose certain methods for their research in questionable cases. We agree that this is a vital addition to all malware research and will be adding that requirement to our projects soon and assessing the moral reasoning used by each researcher.

IV. Conclusion

Given that research ethics in malware studies is often completely overlooked yet their work stands to have immense impact on global society, it is vital that we teach the concepts of research ethics early on in the development of new malware researchers. There are special challenges to this goal as we have seen in this paper, but these challenges can be met and we have provided a case study where malware instructors have successfully inserted ethical training in a course on malware programing.

Acknowledgment

I would like to acknowledge my collaborators in the development of this topic: John Aycock and George Ledin.

References

[1] Trusteer, (2014). Correcting and replacing trusteer partners with california state university on malware research program. Wn.com, Accessed on March 25, 2014 at: http://article.wn.com/view/2014/01/31/Trusteer_Partners_with_California_State_University_on_Malwar/

[2] Young, J. (2009). Top 10 threats to computer systems include professors and students. Education Digest, 74(9), 24-27.

[3] Ledin, G. (2005). Not teaching viruses and worms is harmful. Communications of the ACM, 48(1), 144.

[4] Ledin, G. (2011). The growing harm of not teaching malware. Communications of the ACM, 54(2), 32-34.

[5] Kushner, A. (2008). This bug man is a pest. Newsweek, 152(6), 46.

[6] Wasp, J. (2008). The Dark World of Computer Security. Sonoma Insights, Fall, 14-16.

[7] Kelly-Bottle, S. (2008). All Things Being Equal, ACM/QUEUE, January/February, 55-56.

[8] Chayamiti, I. (2009). Ecola de Hackers, SUPER. Jan, 19-21.

[9] Aycock, J. , & Maurushat, A. (2008). "good" worms and human rights. ACM SIGCAS Computers and Society, 38(1), 28-39.

[10] Aycock, J. (2008). Painting the internet. Leonardo, 41(2), 112-113.

[11] Why "No Worse Off" is Worse Off, http://www.caida.org/workshops/creds/1305/slides/creds1305_jaycock.pdf

[12] Deibert, R. , & Crete-Nishihata, M. (2011). Blurred boundaries: Probing the ethics of cyberspace research. Review of Policy Research, 28(5), 531-537

[13] Buchanan, E. , Aycock, J. , Dexter, S. , Dittrich, D. , & Hvizdak, E. (2011). Computer science security research and human subjects: Emerging considerations for research ethics boards. Journal of Empirical Research on Human Research Ethics, 6(2), 71-83.

[14] Sullins, John, "Information Technology and Moral Values", The Stanford Encyclopedia of Philosophy (Spring 2014 Edition), Edward N. Zalta (ed.), Accesed 3/26/2014 at: http://plato.stanford.edu/archives/spr2014/entries/it-moral-values/ .

[15] Milliken, J., Selis, V., and Marshall, A. (2013). EURASIP Journal on Information Security, volume 2. Retrieved 3/28/2013 at: http://jis.eurasipjournals.com/content/2013/1/2

[16] ACM: Task Force for the Revision of the ACM Code of Ethics and Professional Conduct, ACM Code of Ethics and Professional Conduct. Retrieved 3/27/2014 at: https://www.acm.org/about/code-of-ethics

[17] Peslak, A. R. (2007). A Review of the Impact of ACM Code of Conduct on Information Technology Moral Judgement. Journal of Computer Information Systems. Retrieved 3/27/2014 at: http://web.cs.wpi.edu/~hofri/Readings/ImpactAcmCode.pdf

[18] Moor, J. H. (1999). Just Consequentialism and Computing. Ethics and Information technology 1: 65-69, 1999. Retrieved online 3/27/2014 at: http://www.idt.mdh.se/kurser/computing/DVA403/Lectures-2010/Moor.pdf

[19] Aycock, J. , Somayaji, A. , & Sullins, J. (2010). The Ethics of Coexistence: Can I Learn to Stop Worrying and Love the Logic Bomb? Working paper: TR 2010-986-35, December 2010.