Global Information Assurance Certification Paper

Crossing the Line:

Ethics for the Security Professional

By
Scott Carle
GSEC Practical (v.1.4b)

Table of Contents

Abstract

We often hear of the "hacker"[A] who breaks into a system and steals credit card numbers, releases a destructive worm or maybe defaces a website. What do you think about his actions? Are they ethical? Unethical? I think most of us would agree that this constitutes unethical behavior. What about us[B] though? How are our actions viewed when we, in defense of our clients networks or our own networks, engage in activities similar to the above mentioned hacker. I will briefly talk about several systems of ethics and then we will apply them to situations that we as IT security personnel face. Hopefully this will give you a framework for making ethical decisions within the framework of this job. We will find through this analysis that we have to hold ourselves to an even higher standard than that to which we hold the average computer users or even hackers.

A Basis for Ethical Decisions

Utilitarian Ethics

Jeremy Bentham[1] and John Stuart Mill[2] created Utilitarian Ethics in the 19th century. The basic premise is that actions that provide the greatest amount of good over bad or evil are ethical or moral choices. For example if you told a lie to protect someone's life that would be considered a good ethical choice under the Utilitarian Ethics[3] system. Less harm is done by the lie than by telling the truth and putting a life at risk. Beware though, for this system of ethics leads us down the road of "The end justifies the means" kind of thinking. Over the years since Bentham Stuart created Utilitarian Ethics there have been different interpretations of it. One says that if in a particular situation that the balance of good will be greatest if a particular action is taken then to take that action. The example already given would be appropriate for this variation of Utilitarian Ethics. The next major viewpoint on Utilitarian Ethics would take the stance that it is not the action which produces the greatest good for a particular situation but the action that produces the greatest good 'over all like situations' in a society that should be taken. Going back to our example of the lie to save a life, we would find that with this alternative interpretation we would judge that over all lying is more harmful 'to society and the overall good' than not. This being the case we would not lie to save the life but tell the truth as overall it is less harmful in the long run.

A I use the word hacker here to mean someone illegally breaking into a computer or network or writing a malicious worm or virus. I realize that this is a very media centric abuse of the word and that it is not representative of many positive and legal activities that can be defined as hacking. For the purpose of and within this paper please accept this more limited definition.

BBy us I am referring to network security professionals and network administrators acting on behalf of clients and employers in the defense of IT infrastructure and data.

The Rights Approach

The Rights Approach is based on the principle that individuals have the right to make their own choices. A short list of some of the related rights to choice that you would have under this system of ethics would be right to truth, privacy, the right not to be injured, the right to what has been agreed (such as society's laws being fairly administered for and against us). To judge the right and wrong or moral vs immoral of our actions under this system we would have to ask ourselves how our actions affect these rights of those around us. The greater the infraction our actions cause against those around us the more unethical those actions are. Emanual Kant created this ethical system in the 18th Century. Emanual Kant also as part of this came up with the Categorical Imperative that would tell us that all moral rules that we live by should be universal. For example if it is immoral to lie then you should never lie under any circumstances[4].

The Common-Good Approach

P lato, Aristotle, and Cicero were the beginning of the Common-Good Approach[5], which proposes that the common good is that which benefits the community. That as members of a common body that what is good for that body is good for us. This type of system is where we get health care systems and public works programs. In a practical application of it we would look at our actions in light of how our actions would affect the common good of society or our community. For example stealing would never be ethical because it would damage (take resources away from) society or our community. An interesting note reflecting back to Utilitarian ethics is that in some situations stealing would be the ethical thing to do.

Ethics in Conclusion

The study of ethics as you can see does not give us a clear-cut black and white answer to our problems as computer and security professionals. Your answer as to what is right or wrong can change depending on what system of ethics that you follow. Sometimes even within a single system of ethics your answer from one situation to the next might not be the same. Most definitely what you consider ethical will not always be what someone else considers ethical if they derive their answers from a different ethical framework than you do. A prime example of this is the very hackers[6] that we guard against, or are we guarding against ourselves. This makes it important that as members of our professional community we adopt a common code of ethics that applies to our professional behavior. On the next page are two Codes of ethicical behavior that some computer and IT professionals have adopted.

The Code of Ethics[7]

From "A Guide to Forensic Testimony"

1. Technology is important to modern society.
2. Technologists must take care not to endanger the life, health, safety, and welfare of the public.
3. Technologists should demonstrate competence and due care in their technical duties.
4. Technologists must maintain and update their technical skills.
5. Technologists should avoid conflicts of interest.
6. Technologists should be honest and forthright in their dealings with others.
7. Technologists should be honest about their limitations, acknowledging errors and correcting them.
8. Technologists should refrain from discriminating against individuals based on race, religion, age, gender, or national origin.
9. Technologists should give proper credit to others for their work and honor property rights, including copyrights and intellectual property.
10. Technologists should help the public understand technology and support the professional development of peers.

Ten Commandments Of Computer Ethics[8]

From The Washington Consulting Group and the Computer Ethics Institute

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

Stopping Worms and Automated Exploits by Forced Inoculation!

What would you as a computer security professional do if you had the ability to preemptively stop the spread of a worm by patching or inoculating systems in the wild[CD]? You have the capability to patch a known vulnerability before a malicious worm has the opportunity to take advantage of it. In essence what we are talking about is releasing a worm of our own that isn't malicious but benign.

Ethics

Lets take a look at this proposition through the filters of a few of our ethical systems. “Utilitarian “ ethics could take us down both roads. On the one hand, if releasing a benign worm that patched a vulnerability would benefit us more than it hurt others, then we would be justified. The other competing view of Utilitarian ethics would take is that in general releasing worms has a cumulative negative impact. Therefore we should not do this regardless of the reason or situation of the moment.

The “Rights Approach” ethical system would be much more unequivocal about the matter. The Categorical Imperative would hold that your intent didn't matter but the act of breaking into and modifying someone else's computer with out their consent would be an unethical act against that person. Unethical acts are never justified regardless of the reason.

The “Common Good System” of ethics would give us a radically different perspective on the situation. We are all aware of the cost in general that self-replicating worms have cost us as a community. We have all been affected whether as a nation in dollars of revenue lost or as a company that has been financially hurt in reacting to a worm infecting their systems and affecting their connectivity to the Internet. Or affected as an Internet community of individuals that have been inconvenienced by the slow down or even total loss of service that can be experienced when a new worm is rampantly spreading. Under the common good system of ethics we would balance the benefit to the community vs. the harm to the individual. There is a overwhelming case for the community over the individual in this situation. The individual has their privacy infringed on but no malicious actions are taken against them or their systems. Judged against the potential loss of millions or even billions of dollars in the community

C Consider the “Wild” to be the millions of computers that today make up the Internet. Servers, firewalls, routers and workstations that are connected to the Internet make up this wild environment. Only those computers that you control can be considered non-wild or domesticated systems.

DComputer virus expert Paul Ducklin has used “in the wild” as a definition of a type or category of virus. URL:http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci511204,00.html My definition though similar simply refers to the environment of the Internet that is not under your control to be “Wild”

and countless individual hours of inconvenience that other individuals in the community would have to deal with, and then we could say that this would be a clear decision for the community. No individual's loss of privacy could possibly balance the good that the community as a whole would gain.

Example: Code Red vs. Code Green and CRclean

We all know about the Code Red[9] worm and its variants. Even now long after it was released we see it daily hit our firewalls and reported in our log files. It randomly scans the Internet from infected hosts looking for unpatched IIS web servers on port 80 to infect using a IIS buffer overflow vulnerability.[10] In response to Code Red a German named Herbert HexXer released a counter worm called Code Green. Soon after that MarKus Kern released DRclean, which is another counter worm.[11] Below you can see the release letters that these gentlemen posted to the Security Focus mailing list.

Code Green Release Letter

Herbert HexXer posted to the mailing list on the Security Focus website about his Code Green worm release.

> [12]hello guys ...
> ... i have been developing a code, that should patch the isdapi-filter buffer overflow vulnerability (the vulnerability CodeRed is exploiting) discovered by eEye (walk through the code for details).
> As I am on vacation tomorrow and I don't have the time to exessively debug the code, I posted this code here.
> Perhaps some ppl might learn from this code (eventually someone could finish what I began[debug/testing]).
> Be sure to know what you are doing, as this code uses 'viral/worm' techniques and could potentially cause damage.
> THIS CODE IS DESIGNED FOR EDUCATIONAL PUPOSES ONLY; REMEMBER THAT IT IS ONLY A BETA VERSION.
> I will not take responsibility for any damage that might be caused by this code. Be sure to have understood the code and it's pupose before beginning to play with it. Feel free to modify the code at will, but don't blame me, in case something
> should not work like expected.
> Aloah,
> Der HexXer.
> --
> GMX - Die Kommunikationsplattform im Internet.
> http://www.gmx.net

Drclean Release Letter

Markus Kern also in a posting to securityfocus.com had this to say in his release of Drclean

[13]Since we're at it ...
I wrote something similar a few weeks ago but didn't release it back then.
Well, here it is, may the curious enjoy it.
It's a passively spreading worm that patches the box and removes CRII. After installing an ISAPI filter it infects every host sending Code Red, it does not actively scan for vulnerable hosts which should prevent cisco crashes and all the other side effects of Code Red.
Since my assembler skills are limited the main part of the worm is written in C and only the exploit code is assembler.
It should be obvious that I take no responsibility for what you do with this code. Although it doesn't contain any malicious code don't blame me if you hose your network or system.
-- Markus Kern <markus-kern@gmx.net>
PS: The spreading mechanism is broken on purpose

In releasing the code for these two worms Kern and HexXer acted within ethical boundaries per our discussion of forced inoculations ethics. We should note that neither of these gentlemen actually turned the worm loose on the Internet. What they did was release the code with warnings about the dangers of the code on to the security mailing lists. Turning the code actively loose would have taken them into questionable territory ethically, as it would have put them at odds with our Rights Approach and possibly the Utilitarian systems of ethics. You can see this in the below breakdown of their actions.

- They created this code to fix a vulnerability that Code Red took advantage of.
    - Creation of the code in and of it self is a perfectly harmless activity, given their motivation of creating a method of patching a security hole. They violated no individual's rights and did not impact the community in a negative way by the act of creation.
- They did not themselves use this code on any systems they were not authorized to access.
    - Again this is ethical behavior under all of our ethical systems. They have not infringed upon anyone's privacy or rights.
- They did release it to the general public where someone else could use it in or release it to the wild.
    - This would be the closest that they came to having to make a harder ethical decision. Under Kant's Categorical Imperative this could be argued to be their one unethical act. However under the other systems of ethics this could be argued to be well within good ethical boundaries.
- They did not act out of any malicious intent in creating these counter

worms.

- If we count intent then there is no question that they acted ethically. I see no intent to create harm or disrupt the Internet by releasing their worms to the security lists. Ruffle some feathers by treading in a ethically challenging arena, possibly, but not cause harm.

I think that a little discussion of indirect consequences of actions would be appropriate here. Kerns and HexXer's direct actions have passed our ethical tests. However if we were to judge the potential actions of all who now have access to Kern's and HexXer's code we would find that on average someone most likely did use that code in an unethical manner. Thus the potential indirect repercussions from their actions are high. The possibility of someone modifying their code and inserting hostile payloads and then releasing them is very likely. We need to keep in mind though that these actions are not directly tied to Kern's and HexXer's. Any judgment about the ethical appropriateness should be levied against the individuals actually participating in the unethical activity.

My personal belief is that past a certain point, it is foolish to fear creating something new for worrying about people abusing your creation. An example of this could be the knife. How many people have died by being stabbed to death with a knife? I would hazard a guess that it is a fair number in the last one hundred years. Yet we still use knives everyday to cut our food, open boxes, cut rope and for a thousand and one other beneficial uses. Should the first person that sharpened a piece of metal have said, “No, it might be used to hurt someone”? Rather we should concentrate on what we intend to do with it and what our motivations in making it are as the basis for make ethical decisions about whether it is ethical.

Example: Slammer, Stopping it Cold!

Recently we all saw the port 1434 worm called slammer overwhelm the Internet in just a few hours. One of the analysts that works at the same managed network security company as I do reverse engineered the slammer worm. After finding out how it worked he then created a utility that exploits a port 1433 vulnerability to remotely disable the slammer infected system. In my job we have seen multiple resurgences of this worm on clients networks over the weeks after it appeared. Using this tool, and I will call it a tool, allows us to disable a slammer infected system quickly so that it does not overwhelm the network, firewalls, and IDS devices. The infected system is still running but not able to communicate with the network because it's default route is now gone. It is now sitting and waiting on someone to come reboot and patch it.

At work we have discussed various methods of automating this process. If you have it sit as service on a system on the network it could launch against an infected system as soon as it detected an infected system trying to infect it in turn. The biggest question we ran into wasn't “how to do it?” but whether it was

ethically appropriate to create an automated exploit against vulnerable systems. An exploit that has the capability of removing default routes from them or with a little work by a third party if they have access to the code of putting their own payload in to modify a vulnerable systems registry settings. Our decision based on that conversation was that it was a useful tool and that we should implement it. However we all held reservations as to releasing it openly on the Internet through security mailing lists or posting it on our website.

We did not decide that it would be unethical to do so. In fact it was created as a tool to fix a problem and we had no intentions of using it in an unauthorized manner. We then considered the ramifications of how other people view this same issue. Not all people use the same criteria for making ethical decisions. This is what creates the controversy over proposals to release worms onto the Internet to patch or inoculate systems in the wild or to stop infected computers from spreading a worm.[14] Not all people agree that an action in the Common Good is an ethical action, but rather that it comes down to individual actions that do not trespass against any individual. The Rights Approach supports this view point. In our society, the two major viewpoints are probably the Rights Approach and the Common Good approach; republicans vs. democrats to draw a parallel. As a reputable managed security company we wish any controversy about us not to be focused on our ethics. Therefore, we make a decision that we can live with that is ethical under testing from as many ethical viewpoints as possible. Our conclusion was that we create the tool but do not release it to the general public.

Hack Back! Can and Should I do this?

Ethically, your answer can vary depending on the situation and the ethical system you chose to apply. Under Utilitarian Ethics we could again argue both sides of the question. On the one hand defending yourself against an aggressor would be good if the short-term benefits outweighed the harm. The other side of Utilitarian Ethics would say however that fighting or "attacking someone over the Internet" is overall a net loss on the scales of good and bad, therefore we should refrain. The Rights Approach gets interesting here in my interpretation of it. Under the Rights Approach if I attack someone it would be wrong no matter the circumstances. Under the Common Good system I interpret it to say that attacking would never be an ethical choice nor would counter attacking. The common good is not served by using the Internet as a medium of attack. All to often such as in a DOS[E] attack, the attack will affect many other systems and networks other than the targeted systems. This is overall harmful to the community.

Example: Smurf Attack

Some time ago I was involved in responding to the port scan of a clients firewall.

EDenial of Service attack

Following standard procedures we sent an abuse email to the ISP of the source IP responsible for the scan. The official response from the ISP was a brief email back that was very derogatory and profane. Very soon after that, in a matter of seconds, our company came under a DOS Smurf attack.

Our total response to this incident at the time was to block the attack and gather forensic evidence. We had the capability to hit the attacking hosts and kill the attack that way, but we chose not to do that. Did I mention that upon later analysis of the attack we found no direct links between the ISP and the attacking hosts. The attacker sent spoofed ICMP requests to twenty vulnerable networks with our addresses as the originator.

Ethics

What would our ethical systems had to say about us responding to this attack in kind. Under the Utilitarian System we could have argued that more harm was done to our clients and us by the attack potentially denying our company the ability to provide security services if we had been totally taken down. Therefore we would have been justified by responding to protect our ability to provide services. Under the Rights System we would be acting in an unethical manner to respond by attacking. Also under the Common Good system we would have to make the ethical choice to not respond.

To complicate the situation even more is the fact that all the attacking hosts didn't intend to attack us. The attack was initiated by a third party and directed at us through networks that were vulnerable to being used in such a manner. The owners of these networks were not guilty of any intent to attack us.

In the real world what actually happened is that we did not attack back but gathered evidence and are now working with federal and state law enforcement agencies to legally and ethically respond to this attack. If we had blindly attacked back we would have been guilty of attacking companies that had not originated the attack against us. This would have a negative affect on our reputation as a ethical managed security company. Do you notice again that we touch on how it matters what others believe about our ethics?

Example: DOS ATTACK of World Trade Organization

In December of 1999 the World Trade Organization held a summit meeting. In an attempt to disrupt it a group of hackers calling themselves electrohippies tried to disrupt the WTO website by launching a DOS attack on the server hosting it[15]. In this case the attack was not spoofed but rather launched from the server in the UK that the electrohippies had their own website on.

Conxion, the hosting service for the WTO website, redirected the DOS attack

back at the originating source address. Brian Koref, senior security analyst at Conxion is quoted by Deborah Radcliff in her article on NWFusion.com saying[F] "So we told our filtering software to redirect any packets coming from these machines back at the e-hippies Web server,"

According to Radcliff's article, industry response was mixed with many not approving of the retaliatory tactics. Especially if it is not clear who the attacker was.

Ethics

The Utilitarian System would be fairly approving of Conxion's response. Stopping the attacker from affecting their client would be an appropriate ethical response. Even under the branch of Utilitarian Ethics that is more concerned with the broader aspects of the response rather than the specific incidence would not have as much problem in responding to the attack as Conxion did. Having a clear perpetrator and being able to narrowly target the attacker so that the effects don't bleed over to innocent parties makes this specific incident more clear cut in response. Under the Rights System of Ethics we would still not be justified in retaliating in this case. The Categorical Imperative is very unforgiving of circumstances. The Common Good System in general is going to say that launching Internet attacks is bad for the net community overall.

We can complicate the ethical response to this situation though. By moving to a more detailed look at the response Conxion made. Conxion did not launch an attack on the electrohippies server; instead they simply returned (redirected) the attacking traffic back to that server. If you make this distinction then what they did was not an attack but simply redirecting traffic packet for packet that had been sent to them back to the originating address. If you look at it like this, and I do realize that to some degree this is splitting hairs, you could justify doing so under all the ethical systems. It is no longer you attacking but the attacker, in an almost judo like way, attacking themselves.

Conclusion

We have looked briefly at a couple of different situations that can face us as computer security professionals. I think that the overwhelming conclusion that can be drawn is that we should not retaliate. That in most cases it is unethical behavior on our part to reply in kind. There are many defensive routes open to us to stop the affects of attacks or worms. Gathering evidence and responding through our society's legal system is a unquestioned ethical choice under all the ethical systems we have discussed in this paper.

Another fact that we need to face as professionals providing a service to our

FSee citation 15

clients is that it matters how they perceive our ethical choices. If we release worms on the Internet or launch retaliatory attacks on attackers, many people will say "they are hackers pretending to be a reputable company." We have to work at and be seen as working to a higher standard. Do you think that law enforcement would take seriously any complaint that you filed against someone if you yourself are known for ethically questionable actions? It does matter how others perceive your ethical standards.

I would like to note for the record that I don't think that any one individual should release any worm whether it is beneficial or harmful. Possibly under the Common Good System of Ethics I could support the government or possibly a large community driven organization that is respected through out the industry to, with fair warning, release a worm that would patch vulnerable systems in the wild, thereby inoculating the Internet from harmful worms that would take advantage of this vulnerability. But this would be a choice of the community at large not of any one individual. It should also be done with fair warning so that responsible system administrators have the opportunity to patch their systems themselves.

1University College London, 26 Gordon Square, London, WC1. The Bentham Project.
URL:http://www.ucl.ac.uk/Bentham-Project/index.htm

2The Internet Encyclopedia of Philosophy
URL:http://www.utm.edu/research/iep/m/milljs.htm#Utilitarianism

3Velasquez, Manuel; Andre, Claire; Shanks, S.J.,Thomas and Meyer, Michael J. Thinking Ethically:
A Framework for Moral Decision Making. Issues in Ethics - V. 7, N. 1 Winter 1996
URL:http://www.scu.edu/ethics/publications/iie/v7n1/thinking.html

4Santa Clara University ENGR 019/301 - Ethics in Technology Winter 2002
URL:http://cseserv.engr.scu.edu/NQuinn/ENGR019_301Winter2002/RachelsChap9.pdf

5Santa Clara University http://www.scu.edu/ethics/practicing/decision/approach.html

6Denning, Dorothy E. "Concerning Hackers Who Break into Computer Systems." Paper presented at the 13th National Computer Security Conference, Washington, D.C., Oct. 1-4, 1990.
URL:http://www.cpsr.org/cpsr/privacy/crime/denning.hackers.html

7Smith, Fred Chris; Bace, Rebecca Gurley. A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness New York Addison-Wesley 2002 177-179

8Barquin, Ramon C. "In Pursuit of a 'Ten Commandments' for Computer Ethics" May 7, 1992

URL:http://www.brook.edu/dybdocroot/its/cei/overview/Ten_Commanments_of_Computer_Ethics.htm
URL:http://www.brook.edu/dybdocroot/its/cei/papers/Barquin_Pursuit_1992.htm

9Cert Coordination Center URL:http://www.cert.org/incident_notes/IN-2001-09.html August 6, 2001

10Cert Coordination Center URL:http://www.cert.org/advisories/CA-2001-13.html June 19, 2001

11Middleton, James Vnunet.com News Center URL:http://www.vnunet.com/News/1125206 May 9, 2001

12HexXer,Herbert Security Focus Mailing Lists
URL:http://www.securityfocus.com/archive/82/211428/2003-02-13/2003-02-19/2 Sep 1 2001

13Kern, Markus Security Focus Mailing Lists
URL:http://www.securityfocus.com/archive/82/211462 Sep 1 2001

14Reuters. I.T. Matters. Business World Internet Edition
URL:http://itmatters.com.ph/news/news_08062002e.html August 6, 2002

15Radcliff, Deborah, Network World Fusion, Network World

URL:http://www.nwfusion.com/research/2000/0529feat2.html May 29, 2000