Is hacking a computer crime?

April 11, 2014

> "Hacking is the clever circumvention of imposed limits, whether imposed by your government, your IP server, your own personality, or the laws of physics" St. Jude, 1939-2003

1 Introduction

In the everyday life, the word "hacker" is always associated to the "dark side" of computer science: all common people are afraid that some hacker will read their e-mails, steal their credit card number from an on-line shop-ping site, or implant software that will secretly transmit their organization's secrets to the open Internet.

But today there exists also the other side of the dark side: i.e. the ethical hackers.

Before analyzing an actual scenario in which ethical/non-ethical hackers are posing some issues, I want to remind that the term "hacker" has originally defined as:

> **HACKER: noun**
>
> 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities as opposed to most users of computers, who prefer to learn only the minimum amount necessary.
>
> 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

And we want to conclude this small introduction with some remarkable quotes by Judith Milhon (aka St. Jude), that has been considered by many to be the first woman hacker of the personal computing era.

> Hacking doesn't stop with computers. Every revolutionist is a hacker, hacking the social system. The nerd-heroic Wright brothers hacked bi-cycles before they started hacking airplanes. Ms. Manners, a feminist hero, hacks social interactions. The hacker approach works for every-thing in life. At least, it will make you more likely to analyze the elements of your life. At best it will make you want to transform those elements like an alchemist
>
> Hacking is a martial art - a way of defending against politically correct politicians, overly intrusive laws, bigots and narrow-minded people of all persuasions
>
> Hackers are problem-solving animals

2 Scenario and stakeholders

Let's consider the following scenario:

A bank is managing the interests of all the accounts using a specific software. Let now suppose that an external person is able to access and/or change the code of the software in such a way that a small part of the interests that should go on the customers account, are redirected to a different account. Aware of that risk, in the search for a way to approach the problem, the bank realizes that one of the best ways to evaluate the intruder threat would be to have independent computer security professionals attempt to break into their system on purpose. So the bank hires some ethical hackers.

The stakeholders involved in that scenario are the following:

- the bank
- the bank customers
- the state (that needs to define what is a crime and what is not, through the legislative system)
- the education system (that has to teach the new professionals of ethical hackers)
- the media (that influence the public opinion, so also the bank customers, judgement of computer security people)

3 Ethical issues

The ethical issues induced by the above scenario can be the following:

- Understanding the intrinsic difference between a "classical" fraud and an "electronic" one: this has been posed as an important issue, for example, in the italian legislation about computer fraud. Indeed the usual fraud was defined as "inducing, on purpose, an error acting on the psychic sphere of the victim, inducing a distorted representation of the reality in order to gain a profit". But the computer fraud is quite diffrerent because, even if it is plausible to believe that the "induced error" in the software code, is inducing a distorted representation of the reality (for the software), the computer fraud is actually caused by the wrong assumption of the bank employee that the software is perfoming the right task. So because of this difference, and because of the italian rule of the penal code that stands that the analogy principle cannot be applyied in order to punish a crime, the italian laws has to be updated and integrated with these new kind of crimes. The result of the recognition of this difference is a new law in the penal italian code (art. 640- ter, 1 comma) that says the following "chiunque alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalita su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da Euro 51 a Euro 1032 " (anyone, that is altering in any possible way the behaviour of an informatic or telematic system or acting without any right in any possible way on the data, information or programs contained in an informatic or telematic system or in devices linked to it, causing to himself or to others an unfair profit damaging someone else, is condemned to from 6 months to 3 years of jail, and an amends from Euro 51 to Euro 1032).

- The difficulty of identity verification in the virtual world: this has also been considered an important issue in the italian legislation because the abuse of the administrator right has been recognized as an aggravating circumstance for the computer fraud law described in the previous point. The fact that the criminal can hide his identity while is performing the crime, is embedded in the kind of the crime, and so is different from the disguise that a thief can use during a robbery.

- The power of the media: the problem of associating a criminal meaning to the initial neutral word "hacker" has been basically due to the media, and to the unbalanced attentions that as usual they give to criminal acts in comparison to all the possible good application of computer science. A more balanced and objective approach to technology (and to a lot of other fields) has to be considered in the media exposition of the facts.

- Is it better to share or to hide the knowledge of a security fault? This issue is directly linked to the power of the media described in the pre vious point. For example, let's consider what Farmer and Venema did in December 1993: they discussed publicly, the idea of using the techniques of the hacker to assess the security of a system. With the goal of raising the overall level of security on the Internet and intranets, they proceeded to describe how they were able to gather enough information about their targets to have been able to compromise security if they had chosen to do so. They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented. Farmer and Venema elected to share their report freely on the Internet in order that everyone could read and learn from it. They also gathered up all the tools that they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it. Their program, called Security Analysis Tool for Au- diting Networks, or SATAN, was met with a great amount of media attention around the world. Most of this early attention was negative, because the tool's capabilities were misunderstood: it was thought to be an automated hacker program that would bore into systems and steal their secrets, rather than a tool that performed an audit that both identified the vulnerabilities of a system and provided advice on how to eliminate them.

- Is it right to teach how to hack? In the US it is possible to obtain the ethical hacker certification and it is possible to buy the Certified Ethical Hacker Series. One of the CEO of the company that is selling this product was asked to answer to the following question: "Isn't this knowledge dangerous?". His answer was: "I actually had a wave of fear hit me as I was half-way through reviewing this series. 'We can't sell this.' That was my gut reaction. It's too

dangerous, it teaches too much, it's too powerful. My second thought was, 'We need to sell this to as many people as possible', thinking it safest if the people being attacked know exactly how to attack, and therefore how to protect."

- On which principles can we choose the people that has to be teached for hacking? This issue arise directly from the previous one, and from the consideration that the first IBM's requirement for Ethical Hackers is that they must be completely trustworthy because while testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. The other fundamental rule that IBM's ethical hacking effort had from the very beginning was that we would not hire ex- hackers. While some will argue that only a "real hacker" would have the skill to actually do the work, they feel that the requirement for absolute trust eliminated such candidates. They likened the decision to that of hiring a fire marshal for a school district: while a gifted ex-arsonist might indeed know everything about setting and putting out fires, would the parents of the students really feel comfortable with such a choice? This decision was further justified when the service was initially offered: the customers themselves asked that such a restriction be observed. This is a generalized prejudice that can be accepted by a superficial analysis of the situation and is mainly caused by the impact on the media that a "criminal hacking" act has w.r.t. a "good hacking" act. The pubblic opinion usually prefer to be protected by a person with a "clean" past, rather than a person with a deeper experience but a "dark" past: according to me, this is not a convenient choice in the long run and it cannot be set asa general rule that is applied in all cases.

4 Alternative scenarios

Just as in sports or warfare, knowledge of the skills and techniques of your opponent is vital to your success. As with traditional crimes the local law enforcement agents must know how the criminals make their trade and how to stop them. On the Internet anyone can download criminal hacker tools and use them to attempt to break into computers anywhere in the world. Ethical hackers have to know the techniques of the criminal hackers, how their activities might be detected, and how to stop them.

So, the only possible answer to the problem of computer crimes, is to give to some people the same skills as the "bad guys". But instead of denying the possible utility of take advantage of the ex-hackers experience, in my opinion is better to try to investigate what were the reasons of those people to commit the illegal behaviours. Indeed I think that this analysis has to be done on all the ethical hackers candidate, because the only fact that someone has not yet committed a crime, does not mean that he/she has not the attitude for doing it in the future.

The possible reasons for doing a criminal act are mainly three:

1. personal reward ("they hack your Web site because they can")
2. profit
3. bad/criminal attitude

If the motivations that are guiding an ex-hacker (or anyone else) are one of the first two, using him/her as an educator for the new generation of ethical hacker could be a good choice, because the society can take advantage of his/her experience on the field, just by giving him/her a reward in front of the world (a social/monetary reward). If there is the suspect that the motivation is the third, then the person is not a good ethical hacker candidate nor for teaching neither for learning!

5 References

[1] http://members.aol.com/stjude/pillowbook/

[2] http://www.ibm.com/services/security/intrspec.html

[3] http://mylegalman.wordpress.com/frode-informatica/

[4] http://www.cbtnuggets.com/includes/cbtnuggets.css