Global Information Assurance Certification Paper

Nicolas-Loïc Fortin
Version 1.2f
Original submission

Who is the intruder?

Once upon a time, burglars and bandits were easily identifiable bad guys. Nowadays, with telecommunications and computers appears a new kind of criminals: the hackers. Actually, the word « hacker » refers to any curious person who possesses computer related abilities and a great interest for information technologies. The vast media coverage of various computer attacks, these last few years, has not only helped to popularize the word « hacker » but also, often, to define its meaning. The hackers' community is becoming one of computer passionate capable and likely to attack businesses and governments computer networks.

The lack of uniformity in the definition of the word « hacker » does not help to the comprehension of this highly diversified community. The hackers have various motivations, different knowledge and goals, complicating our understanding of their community. Such a matrix inevitably takes on a social character. The behavioural rules in a virtual world are not different then the fundamental ones in the real world.

In an effort to present the «hackers' community» in the best manner possible, I have consulted some of the contributions made to help create these definitions. The main sources used are some texts by Mr Marc Rogers, from Deloitte & Touche, documentation produced by Shaw, Post & Ruby as well as the community itself. In addition, I have participated in various discussions on Internet sites and forums.

I have found these contributions of the utmost interest because of their respective point of view. Shaw, Post & Ruby propose an enterprise oriented approach; Mr. Rogers, an individual oriented approach while the community suggests its own view on its composition. A table showing some of the types is presented in the appendix.

Therefore, I hereby wish to present a summary of the hackers' community typology, inspired by the various sources I have consulted. As well, I will propose a few comments for each group in a computer security perspective.

The hackers' community: who are they ?

The hackers' community can be divided in three main groups, according to their computer knowledge: first, the script kiddies (low level of technical knowledge), then the crackers (low to regular level of technical knowledge) and finally, the elite hackers (high level of technical knowledge).

The script kiddy is often at the beginning of his teenage years and his main motivation is easy glory. He can be characterized by weak technical knowledge and his need to vandalize (glorification). Quickly, he goes from one target to another, looking for easy kills, without targeting any specific organization in particular. Thus, the script kiddy is often simply looking for the respect he hopes to get from the elite hackers, gaining somewhat of a status inside the community.

The cracker is usually in the middle of his teenage years or so. His technical knowledge is not impressive, if he has any at all. His main motivations are, as for the script kiddy, glory and vandalism. On the other hand, the cracker has or gives the impression of being also motivated by a certain social justice (without understanding its range). Therefore, often, he will justify his actions by Robin Hood's principle, robbing the rich to give to the poor. Contrary to the script kiddy, the cracker will not limit his targets to easy ones. As a matter of fact, he will often try to hit well renown companies or military and/or governmental sites. In so doing, he boosts his ego and prestige.

As for the elite hacker, he is often an adult with a regular job. His level of technical knowledge is much higher, usually working in a highly technical environment. His motivations vary depending on what "side" he has chosen. It goes from security officer (white hat hacker) to industrial spy (black hat hacker) or any other possibility in between (grey hat hacker).

The groups in the community : history and recognition

- **Script kiddies**

The script kiddies' group is the most recent of the three in the hackers' community. On the level of technical knowledge, this group is on the lower rung of the ladder. Mainly constituted of beginners, they expect to become part of the elite, eventually.

We could compare this group to teenagers responsible for vandalism and graffiti, acting in such a manner to feel extreme sensations and hoping to impress the hackers' community in general. One very good example of this is Mafiaboy, a young man right in the middle of an identity crisis.

The media coverage of the feat of arms claimed by the script kiddies has attracted the attention of the general public on the hackers' community capacity to access information databases of various nature (personal, financial, scientific, etc.) or to vandalize, to disturb the regular functioning of electronic systems. Such coverage, sometimes extending to sensationalism, also has the effect of minimizing the meaning of what hackers are, therefore contributing to the problem of understanding the structure of their community, who they are. As well, the group of elite hackers does not appreciate them very much, finding them too "visible" in the media's eye, asking for too much attention to be brought on the community in general by their need for recognition and easy/fast glory.

It is my opinion that by increasing the public's awareness in regards to the rules and laws applicable as well as by working in prevention with internal operations policies and control, the number of such illegal and frivolous acts would decrease, the script kiddies becoming more and more discouraged to even try these operations. In fact, such an education would have an impact on the whole hackers' community activities.

- **Crackers**

The crackers are forming one of the well defined groups of the hackers' community. "Born" in the 1980's, they were the script kiddies of the time, on the level of technical knowledge as well as for the motivations. In the same fashion as the script kiddies, the crackers were motivated by the hope of, some day, becoming a member of the presumed elite. Their way of operating would be what separates them from the script kiddies. The latter work in solo, the former often groups, seaming more structured in their operations.

Their level of technical knowledge is roughly similar to the one of the script kiddies though a bit refined. The crackers are often mistaken for hackers because of their average level of exploits. One of their main activities is software piracy (softwares, music, films, etc). They are the creators of warez sites, responsible for the propagation of illegal copies of softwares or movies. They are pleased when having broken the anticopy protection of softwares like Windows XP, for example, and will even distribute it to the members of their community and to the script kiddies.

Another activity they like to participate in is the creation of modern viruses, demanding more programming then before, since the elite hackers have increased their "level of difficulty". They are often the authors of scripts found on the Internet to help use more sophisticated tools. Seldom they possess the necessary knowledge to create tools or solve problems.
The limit between crackers and black hat hackers (see section below), as far as their motivations are concerned, is quite thin. Generally speaking, the crackers are younger and possess more restricted technical capabilities. Therefore, the possibility of them participating to economic or military crimes is lesser, by far, than it is for the black hat hackers. As a matter of fact, most of the time, the crackers simply borrow principles established by the "elite" without truly understanding the economic and/or social aspect of their actions.

- **Elite hackers**

The group of elite hackers is the oldest group of this particular community. Generally older in age, they are also more experienced and technically knowledgeable than the script kiddies and the crackers. Their motivations are more complex in nature and this group can be divided in three sub-groups according to their value and morals, by using three explicit colours: white, black and grey.

- **First sub-group : "white hat hackers"**

A white hat hacker is quite enthusiastic over technology, being fundamentally very curious and doing all he can to satisfy his interest. Some members of this group are responsible for the birth of the Internet and form the club of those who took pleasure in studying the phone system. The white hat hacker tries to get into the system for the shear challenge it presents. For him, bypassing a system or find its weaknesses is part of the pleasure he is looking.

The most noteworthy type of this group is the one we could qualify "samurai", as much because of their method as for their code of honour. The samurai hackers are often called upon by the police forces to help catch a hacker with less noble intentions. According to Shaw, Post & Ruby, we could include in this group every curious person interested by computers. In an enterprise, they would be the colleague looking into the network or giving the most hip command to use.

- **Second sub-group : “black hat hackers”**

The black hat hackers are members of the elite who have been seduced by the darker side of the Force, to make an analogy with the famous Darth Vader in Star Wars. They often hold positions as spies, industrial spies, cyberterrorists or criminals working for some mafia organization. Many insider dealings are committed by them. They are not different from the conventional criminals except for the tools they use to perpetrate their crimes. The black hat hackers are motivated by the lure of a reward, vengeance or are simply attacking with a Robin hood philosophy. This type of action is often called *hacktivism*, a form of pressuring measure used to see modifications applied.

In today's generally computerized environment of organizations and processes, these kind of people are to be feared. More and more, enterprises depend upon computers and for many of them, a failure extending over a long period of time (more than 48 hours) can be fatal. In such a context, it is strongly recommended to be protected against such people as black hat hackers are always in advance on their knowledge of the conventional market of computer security, therefore presenting a serious threat to enterprises in such a weak condition.

Not enough computer professionals take this kind of person (black hat hackers) into consideration in their daily operations. As a matter of fact, there is a rather curious paradox to be made when comparing computer security to the security of your home, for instance. It seems quite obvious that you should install an anti-burglar system to protect your habitation but such a reasoning does not seem to apply to the virtual world.

As it can be stated from the events of September 11th, the terrorists have a strong proclivity to do damage to the vital centres of the Occident and such a potential threat should be feared. As a matter of fact, it has often happened that crackers have entered sensible systems in the United States, controlling the electricity systems for example (California power grid).

Another great problem faced by big corporations is industrial espionage. In today's world of telecommunications and electronic computer systems, it becomes easier, for a competitor, to gain access to strategic information or even to attack the reputation of its opponent by modifying web sites or the integrity of the networks. There is no more need of a face mask, a gun and to risk your life to rob. The simple use of a PC and an Internet connection are enough to embezzle a bank or an enterprise. Many insider dealings have been done with the help of computers, for example by modifying accounting systems or payroll systems, a problem unfortunately becoming more and more common within enterprises.

We are also noticing an increase of unhappy and/or frustrated employees who are forming the greatest plague a company could suffer of. These « black hat hackers » are employees who believe they are important in the organization and, feeling aggravated, wish to get vengeance. The company's hardware is often their target, presenting a minimum risk if the protection against such acts is low, if present at all. When an employee is terminated, it is often forgotten to lock the key after his leave. Such an omission could prove to be a bigger mistake if the employee in question has a very good knowledge of the technological infrastructure and is able to damage it anonymously.

- **Third sub-group : "grey hat hackers"**

The grey hat hackers are characterized by their ambiguity and pragmatism. In a certain way, they are at the intersection of the choices to be made: which side of the Force will it be ? Therefore, they are hard to track. They could just as well follow the noble principles of the « white hat hackers » but will practice on commercial web sites, as would « black hat hackers », but without criminal intentions.

These hackers form the most populous of the elite hackers' groups. Usually crackers in the first place, they are often in their twenties, students in college or at the university or even young workers with a tight budget. Actually, it is often at this stage that they become pragmatic. Without looking for personal growth like the « black hat hackers », they will have a tendency to profit from the basic commodities and, to some extent, from a certain luxury. For example, they will begin to copy softwares, when lacking money, but will not try to make long term profit from the activity.

Excellent experts in the world of computer security might even be ex-grey hat hackers. Although it is quite controversial, their experience of many behaviours related to black hat hackers helps them to understand their methods and, in so knowing, propose and/or apply appropriate security measure to help protect from possible attacks.

Conclusion

By using the generic term “hacker” to define any person able to use the advanced functions on a computer, it is hard to understand the motivations and the means characterizing the various categories of hackers. The better we understand each group's motivations, the more we will be able to understand their acts.

If we comprehend the place we have to give each group, we will be able to focus our efforts more accurately, by using white hat hackers to help secure our technological infrastructures for instance. As well, coercive actions and a better education will help in reducing the growth of the script kiddies, grey hat hackers and crackers groups. The implementation of laws and an increase in the presence of police force will help to catch the black hat hackers. By understanding that the virtual world is nothing but a reflexion of the real world, it will become possible to adapt our systems according to these new concepts. Nevertheless, a robber, be it virtual or real, will always be nothing but a robber.

Appendix

Analogy by the author with the reality	Actual names in the community	According to Mr Marc Rogers	Accor & Rul
Teenagers vandal, punk	Script Kiddies	Newbie/tool kit	
Old fashion bank robber	Cracker	Cyber-punk	Hackers
Nerd	White hat hacker	Old guard hackers	Explorer
			Good Sa
	Grey hat hacker		
Spy	Black hat hacker	Professional criminals	Career th
Terrorism		Cyber-terrorists	Moles
White collar criminal		Internals	Exceptio
			Machiav
			Avenger

References

Inside the mind of the insider
http://www.securitymanagement.com/library/000762.html
(Shaw, Post & Ruby)

Psychological Theories of Crime and "Hacking"
http://www.escape.ca/~mkr/crime_doc.pdf
(Marc Rogers)

A New Hacker Taxonomy
http://www.escape.ca/~mkr/hacker_doc.pdf
(Marc Rogers)

Modern-day Robin Hood or Moral Disengagement: Understanding the Justification for Criminal Computer Activity
http://www.escape.ca/~mkr/moral_doc.pdf
(Marc Rogers)

The new hacker's dictionary
http://www.tuxedo.org/~esr/jargon/jargon.html
(communauté)

Hacker, 15, charged in Web attack
http://www.freep.com/news/nw/cyber20_20000420.htm
(mafiaboy)

Poking Holes in Microsoft's Copy Protection
http://www.pcworld.com/news/article/0,aid,69203,00.asp
(Windows XP)

FBI Issues Cyberthreat Advisory
http://www.pcworld.com/news/article/0,aid,61764,00.asp
(cyber-terrorisme post 11 septembre)

California hack points to possible IT surveillance threat
http://www.infoworld.com/articles/hn/xml/01/06/13/010613hnprobe.xml
(California power grid hack)

Cybercrime Skyrockets, Say Security Reports
http://www.pcworld.com/news/article/0,aid,54591,00.asp
(white collar crime)

Introduction to Hacktivism
http://www.collusion.org/Article.cfm?ID=109
(Hacktivism)