Understanding the Concept of Gaining Unauthorized Access of Computer Systems

Hacking, Crime and Punishment

Abstract

This purpose of this paper is to explore the consequences of computer hacking and cracking in the United States. It briefly covers the laws affecting computer hacking and their appropriateness. A large section is devoted to the arguments for and against hacking in the attempt to identify the benefits and losses to individuals, businesses, and society as a whole of such activities. The analysis of the pros and cons of hacking is essential in determining the weight of punishment attached to computer security related crimes. Finally a recommendation of what needs to be reviewed and changed, and what is acceptable.

Introduction The predator and the prey

John was a kid. Yet, at a mere fourteen years old he could break into most computer systems. One day, over summer, he was sitting at his computer as usual. Bored, he began browsing through his logs of live IPs. After a couple of port scans, he zeroed in on one. He recognized a few of the ports, 21, 134, and 31337. He recognized the 31337 as the numerical representation of ELEET. Remembering that this is the port that a Trojan horse program Sub7 uses for remote access. He downloaded a Sub7 client and hooked up to this remote unknown remote system. He began looking around and, finding nothing overly interesting, decided to let his victim know what was going on. Sub7 has a utility to hijack the mouse and view the users monitor output. Using this, laughingly, he took control of the users mouse as he was browsing the Internet looking at pornographic pictures. He closed the browser and its plethora of pop-ups then opened up notepad.

He typed in some things to scare his victim, like, This is your mother. Youve been very naughty Richard. He had ascertained his name earlier while carousing his files. Finally, after hed had his fun, he said, You have been hacked by SUB7. Get a virus scanner you idiot. What he did not know was that the computer he had hacked into belonged to that of a 56-year-old lawyer. This particular lawyer, while not technically savvy, knew his rights.

Three months later, after hiring a professional security expert, and numerous communications with his ISP he tracked down his attacker. He went to the police with the evidence, who then

made an appearance at Johns house. John was arrested, taken to court, and sentenced to 6 months in Juvenile Hall.

Issues Do our laws adequately and responsibly deal with hacking

Does the punishment fit the crime?

First of all, is it important for the punishment to fit the crime? The majority of people would say yes, for a variety of reasons. For example, some argue that the more unacceptable the crime is to society, the harsher the punishments need to be to deter others from committing it. Others assert that it is our right to be fairly punished by the constitution, which prohibits cruel and unusual punishment. Whatever the reasons, society has made it clear that it feels that the punishment should fit the crime.

Hacking enthusiasts and civil liberties organizations like EFF have complained that in some cases the punishments far outweigh the crime. They claim that the laws concerning hacking are unfair and the punishments out of proportion with crimes of a similar nature. Law enforcement and politicians believe the punishments to be justified and fair. In the example of John, was he treated fairly by the law. Did his accessing anothers computer, even if all he did was warn the user of a vulnerability, warrant his time spent in juvenile hall?

Does hacking have any redeeming qualities?

While many people perceive hacking as a purely destructive activity, there may be some benefits to it. It may well be detrimental to our society if let run amok, much like a disease. Yet even a disease has its beneficial elements. A disease can strengthen the bodys immune system, which improves the individuals over-all health. If our immune system was not trained by mildly infectious diseases, we would be in poor shape indeed if we caught some particularly nasty one. Are hackers similar to biological diseases, which have their positive traits?

Arguments for and against

Does the punishment fit the crime?

In the state of California, residents are subject to CA Penal Code 502, which states among other things:

Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or makes or copies any supporting

documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

Any person who violates any of the provisions . . . is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment

Combine this with the Digital Millennium Copyright Act, which, according to Jessica Litman, states, every time a work appears in the Random Access Memory of your computer, you are making an actionable copy(Digital Copyright p28), can result in some harsh penalties for seemingly harmless crimes. To put it succinctly, if you simply look at anothers files, you could go to jail for up to three years. The penalty for the same crime without the use of the computer is only one year (CA Penal Code 631).

Yet to many, the prevalence of computer hacking and its disproportionately high cost to individuals, businesses and government justifies the disproportionately high penalties.

In a more serious example, under the Anti-Terrorism Act of 2001, violations of the Computer Fraud and Abuse Act (CFAA) may be considered as acts of terrorism. Under the CFAA, defacing a website or simply spamming another user would result in a mild fine. Yet, after the Anti-Terrorism Act, these offenses are punishable by up to 40 years in prison. This to many is an outrageously high penalty for such a minor offense.

Law enforcement argues that such harsh penalties aide in getting plea-bargains out of suspects. This saves them an immense amount of time and money, which allows them to spend more money on other important issues, like fighting the Drug War or investigating violent crimes. Many times, computer security professionals must be called in to track down the cyber criminal, which costs an enormous amount of money (around a $150 an hour).

A third example is of a Cal Poly student, Paul Reed. Paul ran a port scan using a computer on campus. Under Cal Polys Responsible Use Policy, port scans are prohibited. Checking out a bank for security cameras before a heist is the rough equivalent of a port scan. While robbing the bank is certainly illegal, the act of walking around it looking for cameras most certainly is not. Defenders of the policy argue that by far the most prevalent reason for port scanning a computer is to gain information that is directly used to break into that machine. For that reason, they rationalize port scanning as an offense punishable by expulsion. While Paul was not expelled, he did experience some heavy legal problems.

Philanthropic or Ethical Hacking

IBM defines ethical hacking as hacking to find and fix security holes. Ethical hackers are sometimes employed by companies to perform security audits. More often it consists of individuals or groups cracking networks then informing the administrators of the security flaws exploited. Some companies find this sort of activity beneficial in that is an inexpensive way to identify potential problems. This process may cause some administrative hassle, in that they feel that their rights and privacy have been violated and their resources unjustly utilized. Also, it is sometimes difficult to distinguish the ethical hacker from the malicious cracker. This leads the violated corporation to seek legal action against the hacker regardless of intent.

Some ethical hacking consists of finding errors in products that may be used to gain unauthorized access to systems or information. The ethical hacker then provides this information to the developers and the public at large. This knowledge aids the developers in creating a patch for the exploit. By informing the public of the problem, the hacker gives them fair warning of possible security weaknesses. This also puts pressure on the products creators to fix the problem before too many of its customers are harmed by the flaw. Many corporations complain that this damages their products reputation and costs them in lost revenue.

Increased Security

A consequence of the pervasiveness of hacking is companies are encouraged to maintain higher security standards. This creates the need for more rigorous testing, better design, and a higher level of professionalism in the field if the company wants to keep the trust of its customers. This provides the public with more secure and well-tested software.

The trade-off for the superior merchandise is an increase in costs, a delay in release schedules, and possibly a reduced feature set. This is mainly due to the increased costs of production and operation that results from the heightened security measures. So while end-users may benefit from a more secure product, they may suffer by receiving a less useful product for their money.

Intellectual Growth

Laws that prevent hacking also prevent the intellectual growth of the hackers who frequently push the limits of their abilities through the exploration of systems. The difficulties encountered while hacking challenge the individual to increase his knowledge of all aspects of the target. These individuals frequently go on from their mostly harmless juvenile hacking to become competent technicians and professionals. Companies may then benefit from their expert knowledge of systems to create superior products and offer improved services.

However, this training comes at a cost. Companies must pay for added security in their networks and within their products in order to compensate for the frequent attacks. Therefore,

whatever benefits gained by more experienced staff are lost in the increased cost of operations.

Analysis and Recommendations Finding a Balance

Fitting the punishment to the crime

That defacing a website can constitute as an act of terrorism is a bit extreme. The Anti-Terrorism Act should be repealed or amended so that a violation of the CFAA does not fall under its jurisdiction. The law allows for cruel and unusual punishment of minor law-breakers. Crimes that were previously classified as minor offenses are now punishable by up to forty years in prison. The CFAA was passed into law in 1984, and for seventeen years violations of it were not considered acts of terrorism. Also, since the September 11th attacks did not directly involve any violations of the CFAA, it does not make sense for it to be included in the Anti-Terrorism Act.

Further more, the sentencing for violations of CA Penal Code 502 should be the same as for CA Penal Code 631, as they both deal with the same crime in different mediums. It should be no more illegal to monitor anothers Instant Messenger conversations, as it is to monitor their phone conversations. Whether 502 should be toned down or 631 should be beefed up is another issue. The issues concerning what constitutes a violation of Penal Code 502 are ok as they stand. By simply looking at unauthorized material you are violating the law, so that fact that you may or may not be copying anything is irrelevant.

Accountability

Ethical hacking should be tolerated due to the benefits of increased security. Furthermore, software engineers who are made aware of security bugs from whatever source, should be held liable to a limited extent for damages caused by the exploitation of these bugs. This should be a professional responsibility. Software engineers would be a lot more likely to test their code more thoroughly and quickly patch problems if they knew that they could be taken to court as a result of their negligence. Even if not legally bound, according to the joint ACM-IEEE Software Engineering Code of Ethics, software engineers are ethically obligated to address security concerns and accept responsibility for the failure to do so under sections 3.12 Work to develop software and related documents that respect the privacy of those who will be affected by that software and 1.01 Accept full responsibility for their own work. Making developers liable for damages goes hand in hand with mandatory licensing of software engineers.

Raising the bar

While the Software Engineering Code Of Ethics does mention cost-quality trade-offs in sections 3.01, it states in no uncertain terms: Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. Thus, hacking can be tolerated to a limited extent in that it provides economic incentives for companies to follow the highest professional standards so as to minimize bugs and security holes. These incentives are useful because a software engineer may have trouble convincing his management that the extra time spent in design and testing is worth it in for ethical reasons alone.

Free loaders

Allowing hackers to break into systems in order to become more competent computer technicians and professionals is similar to allowing people to break into stores so they will be better store-clerks or cops. There are other ways of gaining the information. There are numerous hacking contests going on all the time, and it is relatively inexpensive to set up a private network of old machines and practice hacking into them. The costs incurred far outweigh the educational benefits these hackers receive.