Computer hacking research paper

Hacking is a illegal break into computer and network systems, according to the negative meaning of the term popularized by the mass media. However, the term Is also found in the Jargon of at least three major hacker subcultures that are characterized by their distinct historical origin and development and that are centered around different, but partially overlapping, aspects of computers (with deferent ideas about who may legitimately be called a hacker, see hacker definition controversy).

In computer security, which the mass media refer to, it is someone who souses on security mechanisms. Parts of this subculture see their aim in correcting security problems and hence use the word In a positive sense. This use Is contrasted by the different understanding of the word as a person who, in a broad sense, adheres to a spirit of playful cleverness and, In a more specific sense, loves programming. It is found in an originally academic movement unrelated to computer security and most visibly associated with free software and open source.

In a third meaning, the term refers to computer hobbyists who push the limits of their software or hardware. Body: When someone hacks a computer or network system, It’s typically for one of three main reasons: Hacking for fun: Some hackers make attempts on computers, servers or network systems Just for the personal gratification. Others may feel that they need to prove something to their peers or friends, and hack something only for the challenge. Hacking to steal: Another reason to hack a system is to steal information or money. A large portion of hacking attempts fall Into this category.

Banks and large companies are common targets for hacking Jobs, but sometimes smaller companies r even a specific person’s computer are targeted, as well. Hacking to disrupt: There are also some hackers, including hacking groups; that target a company to disrupt business, create chaos and just be a nuisance. These groups often be trying to make a statement with their hacking, demonstrate security inadequacies, or to show general disapproval for the business Itself. Examples of hacking groups that made headlines are Anonymous and Lessee.

Positive side of hacking: Hackers are always very familiar with computer systems and can easily find the security vulnerabilities, but not all hackers do dirty works. For example, some hackers are hired by an organization that trusts him or her to attempt to penetrate networks and/or computer systems for the purpose of finding and fixing computer security vulnerabilities. They are known as ethical hackers. These hackers help examining the system or software using hacking method and tell customers so that they can close the hole and prevent potential losses.

Besides, there are also some hackers called “ grey hat hacker”. These hackers may hack Into a computer system to notify the administrator that their system is vulnerable and then offer to repair their yester for a small fee. They are doing It for a good purpose but still demanding personal gain. It may not be ethical but is neither harmful. Negative side of hacking: Though hacking can be positive, we should never neglect Its negative side. And In destroy data or make the network unusable for those who are authorized to use the network with malicious intent or for personal gain.

If a business website is hacked, it may lose not only essential data but also a great number of customers because the website is not operational during that period. If the website sells productions online, it will suffer more. And the website may even get a bad reputation if it is chosen as crackers' target for many times because some customers think the website is not well designed. Besides, cracking may also cause business or government put additional costs on restoring hacked websites or protecting websites from potential cracking.

While on the individual level, crackers may also able to gain unauthorized access into our computers to steal what we have stored, such as credit card numbers, bank account details, address books or other personal, financial or business information. There are three types of hackers: 1. White hat hacker 2. Gray hat hacker 3. Black hat hacker White Hat Hacker A hacker can be a wiz kid who spends too much time with computers and suddenly finds himself submerged in the world of cyber-security or criminal conspirators.

On the other hand, he can be a master criminal who wants to obtain huge amounts of money for him, or even worse, dominate the world. In the movie Matrix, the concept of hackers changed a bit. Although the agents of the Matrix considered them terrorists, the truth is that they were rebels fighting for the liberty of humanity. Things do not need to reach that extreme, though. We are not at war with intelligent a Chinese so that kind of scenario is a bit dramatic. Therefore, a hacker is an individual who is capable of modifying computer hardware, or software.

They made their appearance before the advent of computers, when determined individuals were fascinated with the possibility of modifying machines. For example, entering a determine code in a telephone in order to make free international calls. When computers appeared, this people found a new realm where they could exploit their skills. Now they were not limited to the constraints of the physical world, instead, they could travel through the virtual world of computers. Before the internet, they used Bulletin Board Systems (BBS) to communicate and exchange information.

However, the real explosion occurred when the Internet appeared. Grey Hat Hackers A grey hat hacker is someone who is in between these two concepts. He may use his skills for legal or illegal acts, but not for personal gains. Grey hackers use their skills in order to prove themselves that they can accomplish a determined feat, but never do it in order to make money out of it. The moment they cross that boundary, they become black hackers. For example, they may hack the computer network of a public agency, let us say, NOAA.

That is a federal crime. If the authorities capture them, say, their handle, and get out without causing any kind of damage, then they can be considered grey hackers. Black Hat Hackers Black hat hackers have become the iconic image of all hackers around the world. For the majority of computer users, the word hacker has become a synonym for social misfits and criminals. Of course, that is an injustice created by our own interpretation of the mass media, so it is important for us to learn what a hacker is and what a black hacker (or cracker) does.

So, let’s learn about black hat techniques ND how they make our lives a little more difficult. Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.

There are five forms of attacks commonly used against computers and networks.

1. Distributed Denial of Service (Dodos) attacks usually aimed at networks by third party systems (typically, compromised systems lacking security that unwittingly become hacker accomplices) focuses on open ports and connections in the network or system they undermine the network by flooding it with requests and “ pings,” thereby causing one or more systems and their resources to shut down or crash major systems usually recover from such attacks easily and completely

2. Trojan Horse software disguised as something else (typically useful shareware or freeware) and so are installed in your system consciously it either contains a “ back door,” (which allows others to enter your system, and do what they want with it, while you’re using the software), or o a “ trigger,” (sets itself off when triggered, either by a date or a time or a series of events, etc. And cause your system to shut down or attack other

computers; can be part of a Dodos attack Spare is a less malicious version (it fills commonly-used form fields for you while also collecting information to send to advertisers and marketing companies) difficult to detect

3. Virus most common primary concern is to replicate and spread itself, and then destroy or attempt an attack on the host system examples include: I Love You; Crazy Boot, Cascade; Tequila; Fro

4. Websites – malicious sites that use known security holes in certain system (ex. N older version of Active had a " hole" that allowed content in any one folder or directory on your hard drive to be automatically uploaded to a web directory or emailed to a receiver)

5. Worm it consumes resources (quietly) until the system finally becomes overloaded and ceases to function a combination of a Dodos and a virus attack usually reproduces as often as possible to spread as widely as they can typically lilt for a certain type of system and is benign to all others commonly aimed at larger systems (mainframes, corporate networks, etc. ; some are built to " consume" data and filter it back out to unauthorized users (I. E. Corporate spies) examples are Sobbing and Modem Conclusion. The word " hacker" carries weight. People strongly disagree as to what a hacker is. Hacking may be defined as legal or illegal, ethical or unethical. The media's portrayal of hacking has boosted one version of discourse. The conflict between discourses is important for our understanding of computer hacking subculture.

Also, the outcome f the conflict may prove critical in deciding whether or not our society and institutions remain in the control of a small elite or we move

towards a radical democracy It is my hope that the hackers of the future will move beyond their limitations and become hastiest. They need to work with non-technologically based and technology-borrowing social movements in the struggle for global Justice. Everything in the world has its good side as well as bad side, and hacking is not an exception. There is no way for us stop crackers doing bad things, but as a future computer engineer, we can always choose to stand on the good side.