Hacking and Hackers – An Overview

***B.Hari Prasad**

*Associate Prof & Head - Dept of MCA, Ballari Institute of Technology and Management
Bellary

Abstract

Hacking is to modify something to make it work for you. For computers, hacking includes fixing programs until they work. Also, hacking includes modifying the computer hardware to make it work better or tuned to the person's wishes. The type of hacking that the media discusses includes breaking into secure systems to determine their weaknesses and to explore them. However, the media only points out the malicious uses for breaking into systems. Someone who sets out to crack the security of a system for financial gain is not a hacker at all. It's not that a hacker can't be a thief, but a hacker can't be a professional thief. A hacker must be fundamentally an amateur, even though hackers can get paid for their expertise. A password hacker whose primary interest is in learning how the system works doesn't therefore necessarily refrain from stealing information or services, but someone whose primary interest is in stealing isn't a hacker. It's a matter of emphasis. This paper discussed the basic information related to hacking and hackers.

Key Words: Hacking, Computer hacking, Hacking types, Hackers and Hackers types

Introduction

"Hacking" is, basically, unauthorized access to a computer or network. It could be the unapproved use of one system to gain access to another system (if the hacker is malicious, once access is gained to a machine or server the hacker could change/delete information- such as altering web sites, planting Trojans, etc.), and it could also mean simply entering a specific computer or network without permission.Simply blocking or disrupting access to a computer/server is not "hacking". This is what's called a DoS (Denial of Service) attack. It differs from "hacking" in that the perpetrator has not actually entered or compromised the system/computer targeted. DoS attacks are like piling junk in front of a door, whereas a "hacker" wants to go *through* the door.

Hacking History

During the 1960s, the word "hacker" grew to prominence describing a person with strong computer skills, an extensive understanding of how computer programs worked, and a driving curiosity about computer systems. Hacking, however, soon became nearly synonymous with illegal activity. While the first incidents of hacking dealt with breaking into phone systems, hackers also began diving into computer systems as technology advanced.

Hacking became increasingly problematic during the 1980s. As a result, the Computer Fraud and Abuse Act were created, imposing more severe punishments for those caught abusing computer systems. In the early 1980s, the Federal Bureau of Investigation (FBI) made one of its first arrests related to hacking. A Milwaukee-based group known as the 414s was accused of breaking into 60 different computer systems including the Memorial Sloan-Kettering Cancer Center and the Los Alamos National Laboratory. Later that decade, the infamous Kevin Mitnick was arrested and sentenced to one year in jail for damaging computers and stealing software. He was arrested again in 1995 for computer fraud and put in jail for hacking Motorola Inc., Sun Microsystems Inc., NEC Corp., and Novell Inc. to steal software, product plans, and data. Mitnick eventually cost the firms a total of roughly $80 million.

Types of Hacking

Inside Jobs - Most security breaches originate inside the network that is under attack. Inside jobs include stealing passwords (which hackers then use or sell), performing industrial espionage, causing harm (as disgruntled employees), or committing simple misuse. Sound policy enforcement and observant employees who guard their passwords and PCs can thwart many of these security breaches.

2) Rogue Access Points - Rogue access points (APs) are unsecured wireless access points that outsiders can easily breech. (Local hackers often advertise rogue APs to each other.) Rogue APs are most often connected by well-meaning but ignorant employees.

3) Back Doors - Hackers can gain access to a network by exploiting back doors 'administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups. With the aid of computerized searchers (bots), hackers can probably find any weakness in your network.

4) Viruses and Worms - Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms attempt

to shut down networks by flooding them with massive amounts of bogus traffic, usually through e-mail.
5) Trojan Horses - Trojan horses, which are attached to other programs, are the leading cause of all break-ins. When a user downloads and activates a Trojan horse, the hacked software (SW) kicks off a virus, password gobbler, or remote-control SW that gives the hacker control of the PC.

6) Denial of Service - DoS attacks give hackers a way to bring down a network without gaining internal access. DoS attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).

Distributed DoSs (DDoS5) are coordinated DoS attacks from multiple sources. A DDoS is more difficult to block because it uses multiple, changing, source IP addresses.

7) Anarchists, Crackers, and Kiddies - Who are these people, and why are they attacking I your network?

Anarchists are people who just like to break stuff. They usually exploit any target of opportunity.
Crackers are hobbyists or professionals who break passwords and develop Trojan horses or other SW (called warez). They either use the SW themselves (for bragging rights) or sell it for profit.

Script kiddies are hacker wannabes. They have no real hacker skills, so they buy or download warez, which they launch.

Other attackers include disgruntled employees, terrorists, political operatives, or anyone else who feels slighted, exploited, ripped off, or unloved.

8) Sniffing and Spoofing - Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister.
Spoofing is the act of sending an illegitimate packet with an expected acknowledgment (ACK), which a hacker can guess, predict, or obtain by snooping.

As the cost of hacking attacks continues to rise, businesses have been forced to increase spending on network security. However, hackers have also developed new skills that allow them to break into more complex systems. Hacking typically involves compromising the security of networks, breaking the security of application software, or creating malicious programs such as viruses.

The most popular forms of network hacking are denial of service (DoS) attacks and mail bombs. DoS attacks are designed to swamp a computer network, causing it to crash. Mail bombs act in a similar fashion, but attack the network's mail servers. When eBay was attacked in February 2000, its Web server was bombarded with fake requests for Web pages, which overloaded the site and caused it to crash. Network hackers also try to break into secure areas to find sensitive data. Once a network is hacked, files can be removed, stolen, or erased. A group of teens in Wichita, Kansas, for example, hacked into AOL and stole credit card numbers that they then used to buy video games.

Application hackers break security on application software-software including word processing and graphics programs-in order to get it for free. One way they gain access to software that requires a serial number for installation is by setting up a serial number generator that will try millions of different combinations until a match is found. Application hackers also sometimes attack the program itself in an attempt to remove certain security features.

Computer Hacking

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Since the word "hack" has long been used to describe someone who is incompetent at his/her profession, some hackers claim this term is offensive and fails to give appropriate recognition to their skills.

Effects of computer Hacking

1. Computer hacking is the break of computer security. It exposes the sensitive data of the user and risks user privacy. These activities disclose the secret user information such as personal details, social security numbers, credit card numbers, bank account data, etc. This can lead to illegitimate use and modification of users' information.
2. Modification of important data with intent to achieve personal gain is another effect of computer hacking. This can lead to the loss of all the data stored in the computer. The modification of sensitive data is a worst effect of hacking.

3.Another significant consequence of hacking is identity theft. This fraud involves pretention to be someone else, with determination to gain unauthorized access to information property. It meant to be an illegal use of someone else's identity for personal use.
4. With the advancement in technology, several key-logging software have been evolved which are capable of tracking and recording key stroke by the user, causing stealing of passwords and account details. Another ill effect of computer hacking is the refusal of service attack. This refers to the DOS attack, which makes computer resources inaccessible to authorized users. Often, websites fall prey to denial of service attack which causes unavailability of them for longer period of time.
5. Computer hacking can also cause theft of significant business information. This can disclose email addresses to hackers which could be used by them to use it for spamming and destroying email privacy.
6. If the information related to national security, confidential government data, information related to national defence and security, if exposed by mean of hacking can lead to severe consequences.
7. Hacking can be used to convert computer into zombies. Zombie computers are used by the hackers for fraudulent activities.
Most of the hackers are less noble and use their skills to steal personal information. But this type of computer hacking can sent them to a federal prison for up to 20 years

Hacking Method

There are various methods "hackers" use to gain access... most involve protocols that computers utilize to share information with each other. Even a home computer can be used to host a web site; enabling HTTP and FTP protocols on a home computer allows people, at various levels of access (depending on the host computer's configuration), to browse around inside the host computer whenever it is connected to the Internet.
In many sites on the Internet, there are utilities available to assist in "hacking". It's no longer a pastime strictly for programmers and other script-savvy individuals.

Hacker

A hacker is a person who legally breaks into a computer system to identify the security flaws in that system. A hacker is someone companies hire to enter such systems and resolve these issues. People who hack into computer systems with malicious intent are actually known as "crackers"--this is not hacking

Review

Steven Levy's book Hackers first codified the Hacker Ethic. As noted earlier, there are two key principles that relate to computer security: freedom of information, and a mistrust of authority.

Depending on the interpretation of these principles can lead hackers to define themselves as white or black hat, or variations of grey in between.

To a typical white hat, freedom of information implies a number of things: public disclosure of vulnerabilities, . It is also not interpreted to mean that all information, including private nd personal information, should be free. When the ethic was devised, few people had large amounts of personal data available online, and many of the core ideas of personal computing were impractical or impossible.

There are also a number of documents referred to as “The Hacker Manifesto.” The first such
document was written by Loyd Blankenship (under the screen moniker “The Mentor”) and as
published in Phrack in 1986 under the title “The Conscience of a Hacker.”
While it has fairly dark and anarchistic overtones, it has inspired an ethical basis for hacking in many readers, even appearing in the movies Hackers. It is important to note again that this literature may have inspired just as many if not more black hats, and it cannot be regarded as strictly beneficial in nature. Other influential documents show a trend towards further disorder.
Another document, simply titled “Manifest,” elaborates on the themes of anarchy and alienation. To be sure, many may find in these documents the inspiration to hack for the sake of hacking, which can easily lead to—or be construed as—black hat.

There are many hacking-related periodicals, such as Phrack and 2600. While the information may often pertain to explicitly black hat activities, there are also altruistic motives behind some of the writing. A white hat must surely be familiar with the literature to remain informed on hacking-related developments, and may even contribute to increase the awareness of exploits and other information that should be "free."

Function

Hacking is an activity that is engaged in by people who use their knowledge of the internet, computers, firewalls and security preferences to break into other people's computers, allowing them to view private information, alter data and steal files, information or programs. MySpace pages, software applications and email accounts are the most common programs that are hacked into. Hackers typically look for passwords or credit card information.

Some will simply hack into these programs in order to change information, such as a screen name, password or other content that is written by the owner.

Significance

Hackers are sometimes motivated by greed and steal personal information in order to take on someone's identity for their own gain, or in politics, where they try to exploit, blackmail or otherwise expose someone in power, or even just for entertainment, where hackers simply want to see what they are capable of doing. These types of hackers usually brag about their conquests on message boards or instant messaging programs, competing with fellow hackers as to who is the best among them.

History

The first case of hacking occurred in the 1960s when a group of students at the Massachusetts Institute of Technology (MIT) tried to access the school's main computing systems.

In the 1970s, "phone phreaks" hacked into telephone networks and made toll-free calls. Mainstream computer hacking as we know it today gained momentum in the 1980s when hackers broke into what would now be considered message boards. Congress passed the Computer Fraud and Abuse Act in 1986, which made it illegal for anyone to break into anyone else's computer system. Despite the law, the 1990s saw the invention of the Trojan Horse, which allowed hackers to access any computer that downloaded the program. Many companies were hacked into as well, such as AOL, Yahoo!, Amazon and eBay.

Types

There are at least five main types of hackers. A hacktivist uses his hacker skills in order to broadcast a political message on the Internet. A cyberterrorist commits acts out of a desire to wreak havoc and cause harm to groups who he feels oppose him and his beliefs.

A black hat typically breaks into a network in order to obtain information that will allow him to commit fraud or theft. A white hat may commit the same hacking acts as other hackers, but is not motivated by a malicious intent. A script kiddie uses hacking software in order to break into someone else's computer system. This software is usually obtained from another hacker who has figured out how to corrupt that specific program's system.

Features

Most hackers are talented computer programmers. They know how to write software and how to remove the kinks from other programs that are written by the hacking community. The most important feature of someone who hacks, however, is the "hacker mindset," a set of beliefs that the hacker community has established. The core belief is that it is OK to hack into someone else's computer and to obtain, distribute or otherwise exploit any information that may be found in the process. Hackers usually strongly believe in their First Amendment rights and believe that hacking falls under this umbrella.

Conclusion

Hacking is a recent technology; it affects the computer in several ways. A hacker has always been someone who pushes the bounds of technology. Generally they have been affiliated with the open source movement and have been known to put some of their work in the public domain. As computing has evolved, we have seen a move away from innovations in hardware, and onto software, and now onto the Internet. Based on history we see that newer fields of computing are generally the places where hackers have the largest impact. This would lead to the conclusion that the impact of hackers will be felt most in the developments to do with the Internet in the short term, and in the medium term it would seem inevitable that other newer fields of computing would attract the interest of hackers. There is already significant buzz surrounding sensor networks and motes, so it would not be surprising to see a large amount of innovation in these areas.

References

http://www.articlesbase.com/security-articles/effects-of-computer-hacking-1521016.html
http://www.wisegeek.com/what-is-computer-hacking.htm
http://www.ehow.com/how_2104644_hack.html
http://www.ehow.com/about_4588504_hacking.html
www.Donwload.pconverter.com
http://wiki.answers.com/Q/What_are_the_types_of_hacking

http://mitnicksecurity.com/media/2005%20FBI%20Computer%20Crime%20Survey%20Report.pdf 2005 FBI Computer Crime Survey Report

http://www.usdoj.gov/criminal/cybercrime/cclaws.html Computer Crime & Intellectual Property Section, United States Department of Justice