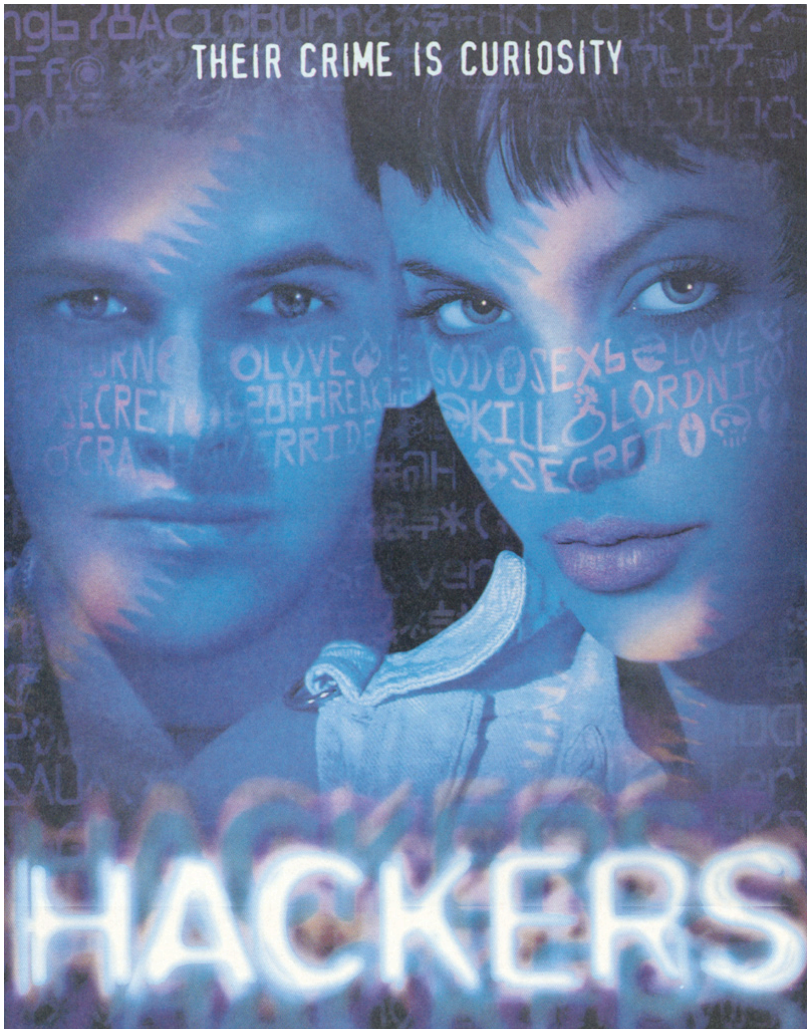
Section 1: Geeks, Hackers, and Crime



A Discussion of Technology and those who use it for criminal gain

Lecture Outline

I. Geeks, Early Adoption and Crime

II. Hackers

III. Other types of Cyber “criminals”

IV. Hacker Subculture

V. Types of Hackers

VI. Famous Hackers and their crimes

What is a Geek?

What is a Geek and why does it matter to crime?

They are those who have chosen to focus on technical skills, generally with computers, over social acceptance.

<u>Geek Characteristics</u>

Gamers: Both computer and role playing games

Science fiction fans, with an affinity for Star Trek

Computer Programming ability

Early adopters of technology

Early adoption of technology is a key aspect of crime

Early Technology Adoption

Early adoption is the phenomenon of acquiring the newest technology as soon as it is available, or sometimes before availability, in the general market.

Much of the technology is adopted later by the mainstream, as early adoption is very expensive and often filled with “beta” problems.

Often focused on gadgets, but it can also be a focus on utilitarian technology.

Historical Examples

CD, DVD, Personal computers, internet, Broadband, VOIP, EVDO, e-mail, digital cell phones, GPS, etc..

Criminals are often early adopters of technology, using it to exploit society in general for criminal gain.

Crime and Early Technology Adoption

Criminals have always exploited new technology for their benefit in committing crime.

Importantly, police often lag well behind criminals in ALL aspects of technology and are thus caught at a disadvantage.

Historical Examples:

1. Cars: Used in bank robberies.
2. Machine Guns
3. Personal Computers: First used for money laundering and fraud, as well as other crimes.
4. Cell Phones
5. Internet: Distribution of goods, communication, anonymity.

Unintended consequences of early adoption of technology by criminals

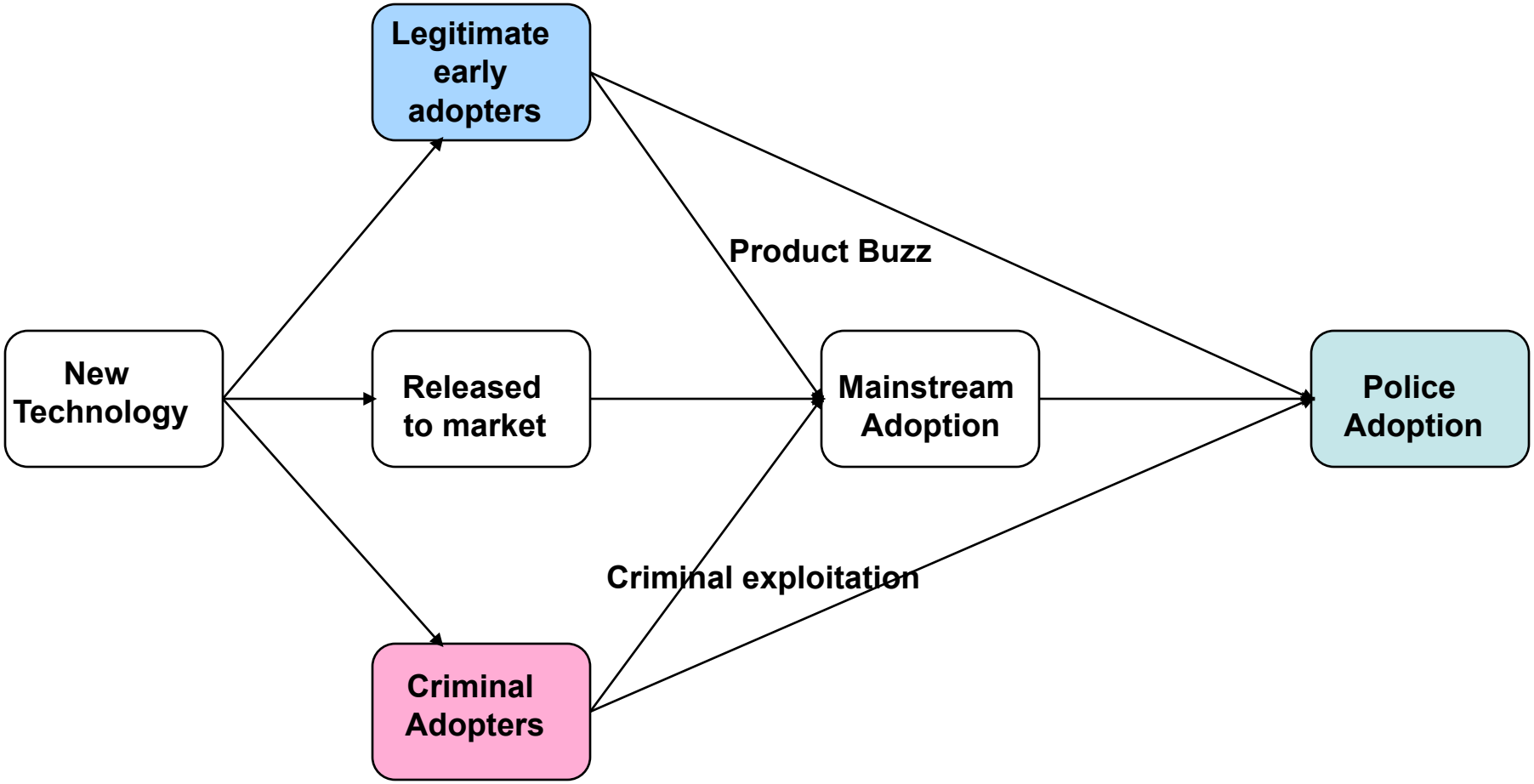
While criminals often have a great advantage at the beginning of using new technologies, the long term effect has actually been very beneficial to society in many ways.

1. **Beta Testing**: Criminals through there exploitation of a new technology often find the problems with it before it makes it to mainstream society.
2. **Innovation**: New products are developed that can not be so easily exploited for criminal use.

   Digital cell phones are harder to intercept than analog

3. **Cost of Goods**: Lowers prices as demand increases.
4. **Economic Engine**: Fighting criminals and malicious uses of technology has become a major part of business and economy.

Technology Adoption Timeline



Hackers

Are Hackers criminals?

Not necessarily, but popular media and myth has made the term into one synonymous with criminal.

Originally Hacker referred to an unorthodox problem solver and master programmer.

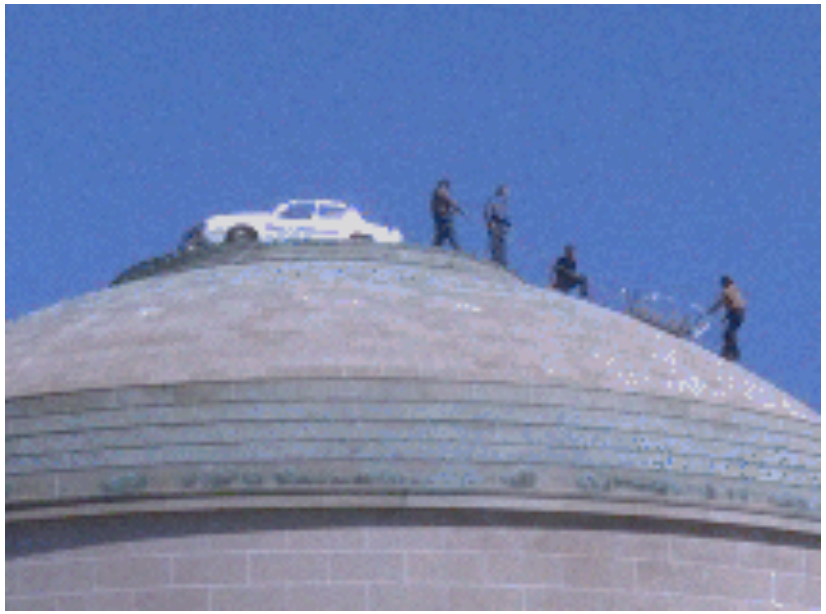
Early hackers made the first computers and the programs that are vital to modern society.

Bill Gates, Steve Jobs, Gordon Moore

MIT claims to have been using the term since before computer hackers existed to describe the elaborate college pranks that are a tradition at MIT.

Early “hacks” were about fun, innovation and style more than anything else.

MIT Hacks

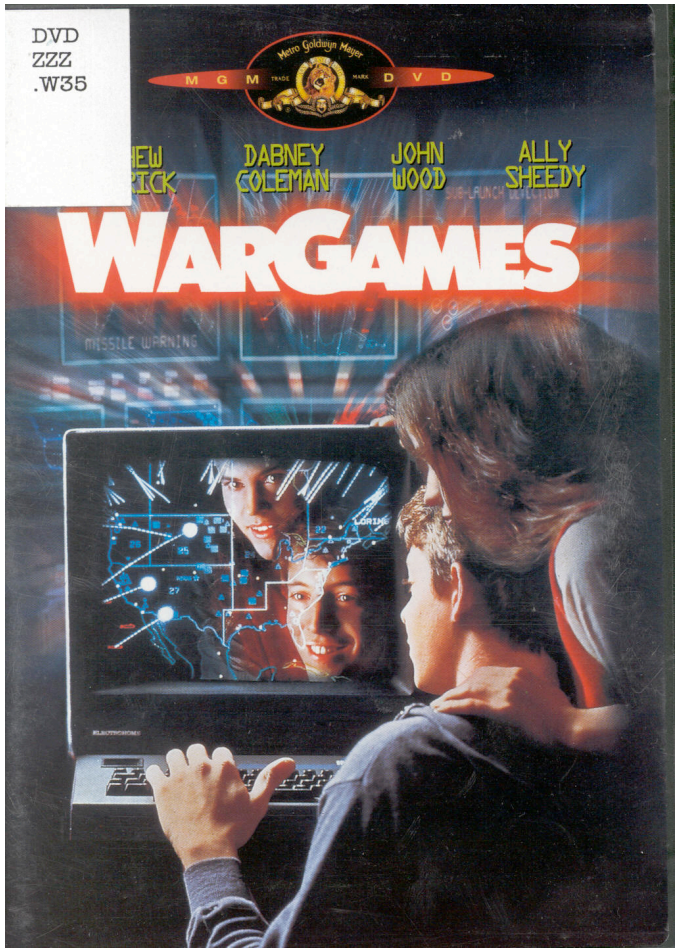


Replica police car built on Great Dome at MIT

Propeller hat on Great Dome at MIT

Change in Hackers

The term Hacker first gained its criminal perception in the early 1980's after the movie "War Games", which inspired a mini-boom in amateur hacking copy-cating the movie.



Change in Hackers

The term Hacker first gained its criminal perception in the early 1980's after the movie "War Games", which inspired a mini-boom in amateur hacking copycating the movie.

Several celebrated cases of hacking occurred in the years directly after the release of the movie, all attributed to teen hacker groups.

While traditionally hackers, such as those at MIT, didn't worry about breaking laws, the new generation of hackers has been defined by law breaking.

Because of this there has been a fierce debate within the hacker/computer world about the use of the term hacker to identify someone who is a criminal

As a result there have been several different terms created to differentiate between hackers and criminals.

Hacker Ethics

Essential to understanding different types of hackers and computer criminals is a basic understanding of hacker ethics

- Do not profit from intrusion
- Do not intentionally harm a computer system
- Attempt to inform a system administrator of security flaws
- Hackers are not bad guys; computer criminals are bad guys

Importantly, these are not established ethics that all hackers must adhere to or even acknowledge.

These are a few very simple rules that some hackers live by

Variations on a Hacker Theme

Within the subculture of hackers there is a distinction between different types of hackers and criminals that is based largely on motivation and end results.

Importantly, these distinctions are subtle and generally missed by the larger culture, but are very important to the hacker subculture.

In particular hackers who do a malicious hack simply to further a crime are not respected by much of the hacker community.

However, if the hack demonstrated great technical skill and embarrassed law enforcement or the government, the hacker would be viewed with great status.

This difference in status can greatly impact investigations into the incidents.

Variations on a Hacker Theme

Computer Criminal: General term for those who use computers to commit a crime.

Differs from hackers in their motivation for the act.

Importantly, hacker subculture does condone some criminal hacking, as long as the motivation is good or pure to the hacking spirit.

Cracker: The established term for a malicious hacker that is favored within hacker circles.

There is no good established criteria for determining the difference between a cracker and a hacker.

Variations on a Hacker Theme

White Hat Hacker: This term is used to describe an ethical hacker.

The term came about largely after reformed hackers moved into the legitimate business and consulting world as a means of distinguishing them from those who were illegal.

White Hat Hacking

- Software testing
- Independent verification of software security
- Reverse engineering
- Training

White hats are often hired to test the security of new networks and security systems for companies

Variations on a Hacker Theme

Black Hat Hacker: This term is used to describe a cracker or malicious hacker.

Importantly, this term does NOT apply to all computer criminals.

ONLY network intrusion and other “hacker-like” activities committed in conflict with hacker ethics qualify as black hat activities.

Originally the term was coined by those outside of the hacker community, but has since been adopted by hackers to describe themselves.

Variations on a Hacker Theme

Gray Hat Hacker: This term refers to someone who usually behaves in an ethical manner, but sometimes violates accepted ethical standards.

Think of this as the “party-smoker” of hackers.

A typical Gray hat hacker is someone who is a penetration tester who doesn’t go after his own clients, but occasionally hacks and intrudes on other networks for fun.

Penetration testing for profit is also frowned upon by some hackers as a violation of hacker ethics.

In addition to network intrusion for fun, Gray hat hackers may also do some other criminal things for profit.

Penetration Testing

This is a type of security analysis where hackers will attempt to break your system in order to help you figure out where any potential vulnerabilities may lie.

This type of work is often scorned by hackers as profiting from hacking and is also disliked because of its sometimes close relationship with law enforcement.

Key Issues in PT

•Information discovered in the testing MUST NOT be disclosed to anyone but the employer.

•Only intrude where invited.

•Loyalty to the employer is essential for business survival.

White hats often associate with black hats to stay current.

PT Company DEFCON

Hacker Subculture

As with other subcultures, the hacker subculture is one that is borne out of feelings of being an outsider or different from the mainstream.

Central to the hacker subculture is the computer.

Everything in the hacker subculture revolves around the computer, it is the god of their religion.

The “outside the mainstream” nature of the subculture coupled with the focus on all things computer has shaped the rules behavior, status, and ethics of the subculture.

Hacker Ethics-Traditional Ethical Standards

1. Access to computers--and anything which might teach you something about the way the world works--should be unlimited and total.
2. All information should be free.
3. Mistrust authority--promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

Hacker Ethics- Newer Ethical Standards

As with most things that involve culture, the ethics of the hacker subculture are constantly evolving.

This is an updated version of hacker ethics which stresses information sharing and doing no harm.

1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source and facilitating access to information and to computing resources wherever possible.
2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality.

**Hackers generally self-regulate, in that they often stop "wannabees" from doing bad or criminal things.

Hacker Characteristics- A hacker is…..

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it
or on it; as in `a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. A malicious meddler who tries to discover sensitive
information by poking around. Hence "password hacker", "network hacker”.

From http://www.mithral.com/~beberg/hacker.html

Hacker Characteristics- A hacker hates

IBM mainframes.

Smurfs, Ewoks, and other forms of offensive cuteness.

Bureaucracies. Stupid people. Easy listening music.

Television (except for cartoons, movies, the old "Star Trek", and the new "Simpsons").

Business suits. Dishonesty. Incompetence. Boredom. COBOL. BASIC. Character-based menu interfaces.

Anything Microsoft.
From http://www.mithral.com/~beberg/hacker.html

1337 Language

As is often common within a subculture, hackers have their own language.

The language is known as “1337” or “leet” which is short for elite.

The language gets its origin in the Bulletin board systems or BBS that were popular among hackers before the internet and chat rooms.

The purpose of the language was twofold:

1. **Speed**: BBS systems didn’t have much bandwidth and typing more than necessary was avoided.

   Similar to texting

2. **Secrecy**: Typing notes in 1337 speak was a good way to keep non-hackers from being able to understand it.

   Essentially it was a form of code.

**Importantly, many “true hackers” avoid 1337 speak, refering to it as the sign of a noob or poser.

More often than not, 1337 is used on forums and on t-shirts.

1337 Quiz

1337 5p34k:	Leet speak
haxx0r:	Hack
fuxx0red:	f**cked up. As in I fuxx0red their system up
phjear:	Fear, also written ph33r
n00b:	Newbie or wannabee
pr0n:	Synonym for porn, a major hobby for some hackers
Flame:	Abuse someone.
pwn:	Own someone, as in I pwn you
suxx0r:	When something sucks.
w00t:	happy, yea

Hacker Cool

As with any subculture, hackers have their own version of what is cool and socially acceptable.

In the hacker culture, movies play a central part in the social scene and there are several movies which help to define and enculture new hackers.

Hacker Movies

Real Genius

WarGames

Hackers: Love/hate relationship

Tron

Matrix Trilogy: First is considered the best

Hacker Typology

While these are not typologies that are often used amongst hackers, they are a good, general way to differentiate amongst the various different kinds of hackers.

This is one version of a list of all Hackers and there are several others that may discuss other types and have other characteristics.

Each will be discussed in terms of their skills, resources and enculturation into hacker culture.

1. Old School Hackers
2. Bedroom Hacker
    A. Larval Hacker
    B. Warex D00dz
3. Internet Hacker
    A. Script Kiddies
    B. Hacktivists

Old School Hackers

Originated at MIT and other schools of that caliber in the 1950's.

All hackers existed solely at Universities and research areas as no one else had computers at that time.

Skill

They are the ones that wrote the book on computers, computer programming, etc..

Skill is unmatched in many ways, primarily programming.

Resources

Unlimited access to computer hardware, but resources weren't that impressive.

Enculturation

Very high, as they created the culture that has evolved.

Programming skill is huge source of status, particularly being able to write simple efficient programs to solve complex problems.

Strong desire to have information to be free.

Bedroom Hackers

Came about in the 1980's as personal computer use exploded.

Skill

Skills are below those of old school hackers, but there are some "elite" hackers that are good.

Skills are more suited to intrusion and internet related hacks.

Resources

Limited resources as they are on a "lawn-mower" budget.

Very powerful computers were still largely at Universities and research companies

Enculturation

Willing to do what they needed to get the "knowledge" they craved.

Often did illegal things to gain access to answers they sought and computers resources they needed.

First to commit crimes in the name of hacking.

Phonephreaks, etc..

Larval Hackers

Sub-group of bedroom hackers that came about in the internet age after the bedroom hackers

Most of their information about hacking comes from media and they are more prone to get involved in cracking.

Skill

Limited skills, but very enthusiastic about being a hacker

Always want to prove their skills, regardless of how good they are

Resources

Good access to resources as computers are cheaper, faster and ever more connected than earlier generations.

Enculturation

Unsocialized in hacker ways and culture, they got the “Hollywood” version only.

Socialization traditionally took place through communication with older more experienced hackers. That has broken down over time.

Warez D00dz

Sub-group of bedroom hackers that trades pirated software.

While other groups value exploration and discovery, they value the acquisition of massive amounts of software with broken copy protection.

They value “cracks” and the status it brings them

Skill

Some are very good at cracking copy protection, while others manage fast sites for downloading software.

Skills can range from extensive to non-existent, even for “elite” warez D00doz

Resources

Good access to resources as computers are cheaper, faster and ever more connected than earlier generations.

Enculturation

Developed a separate culture that values a narrow area of software acquisition and breaking of copyright protection.

Not very involved with the traditional hacker culture or its ethics.

Warez D00dz

Of all the groups that are out there currently, this sub-culture is probably the strongest and largest.

This is due largely to the fact that many kids have grown up feeling entitled to software and have developed a disdain for having to pay for software they feel is over priced.

Moreover, this disdain has also been fueled by the download market that sprang up in the late 1990's and allowed people to download anything for free.

Importantly, Warez D00dz have expended out from just software to include:

- Music and movies
- MP3s: volume counts
- Compressed movies: 0 day release
- Cable and satellite descrambling
- DVD decoding
- Peer-to-peer networking
- Console games

Internet Hackers

Combination of old school and new school hacker cultures.

They retain some of the old school values of open-source, with the new school values of cracking, disruption and making money off their skills.

Skill

Possibly the most skilled in the history of hackers due to the wealth of information at their disposal through the internet.

Skill comes somewhat from internet and its unlimited sources of knowledge.

Resources

With powerful computers and fast ubiquitous internet access they have plenty of resources at their disposal.

Information dissemination is key for them, fast and universal.

Enculturation

Enculturation is uncontrolled and haphazard due to information overload and chaotic nature of the internet. Not teaching as much as directing to sites.

Anyone who wants to learn simply Googles and uses trial and error.

Script Kiddies

Often considered a scourge of the internet because they are not that skilled but think they are.

They often go for easy and unskilled attacks, very un-hacker.

Skill

Basically they use pre-made scripts or tools because they don't have enough skill to write their own stuff.

Resources

With powerful computers and fast ubiquitous internet access they have plenty of resources at their disposal.

Without the ability to download already created tools and scripts they would not exist. They don't have the desire or ability to learn to do it themselves.

Enculturation

They don't have the skill of better hackers, but they revel in the damage they can do with their limited skills.

Little organization beyond small groups. They think themselves hackers.

Hactivists

Term first created in the late 1990's to describe hackers who use their skills as a form of protest against those they perceive to be wrong.

Key to hactivists is that they have a political message.

Skill

All over the place from very little to off the chart.

Some groups, such as the Cult of the Dead Cow have been instrumental in helping those in China gain access to filtered content.

Resources

With powerful computers and fast ubiquitous internet access they have plenty of resources at their disposal.

Enculturation

Double encultured in the values of hackers, although slightly skewed, and in political activist culture.

Hacktivist site

Paulsen Hacker Categorization

This is a hacking categorization that I created based on my own research into hacking and hacker culture.

This hacker categorization is based on

1. **Appearance**: While, all hackers hate to be judged on their appearance, they often purposefully dress to annoy or send a message.
2. **Skill**: How much technical skill they have with computers.
3. **Motivation**: What is their motivation for being a hacker.

<u>Categories</u>

Fanboys

IT Guys

Hardcore

Old School

Fan Boys

These hackers are generally considered “wannabees” for their strong desire to try and be a hacker.

These hackers are more into style than substance.

Appearnace

These hackers are all about the “hacker style” and trying to look the part of a hacker to the mainstream society.

Style can be considered a cross between gothic and punk.

Skill

This group has the least amount of skill of all of the groups in this categorization.

Skills are basic although there are some who are quite talented

Motivation

Mostly concerned with looking and acting like a hacker than on being a real hacker.

Complete focus on fooling mainstream as hackers are now somewhat cool

Often a phase they go through

IT Guys

These hackers are generally considered as the college educated hackers who inhabit the IT jobs throughout business.

Don’t consider themselves hackers but “computer professionals”

Appearnace

Dress very differently from other other categories in that they dress mainstream or almost preppy.

Try to fit into mainstream society in most ways

Skill

This group has a great deal of skill, although it is almost completely focused on legitimate computer skills such as system administration and coding.

Motivation

Mostly concerned with making a legitimate living

Least likely to commit a crime, because of the stakes in conformity that they have.

Hardcore

These hackers are generally considered highly skilled in computers and highly encultured into the hacker subculture.

These are the guys who determine what hacker culture is

Appearnace

Black t-shirts and jeans, closets full of black t-shirts and jeans.

Newer hardcores tend to be a little more wild in their dress (piercings, tattoos, etc..)

Skill

This group has a great deal of skill, much of which is focused on illegitimate means of doing things.

Dedicated to figuring out how things work regardless of whether or not doing so is legal.

Motivation

Often have legitimate jobs, but they love to “hack” into things on their time off.

No criminal intent in their actions.

Old School

These hackers are generally considered highly skilled in computers, but not so schooled in social ways

They are born hackers and don't try to get into the subculture.

Appearnace

Black t-shirts and jeans, closets full of black t-shirts and jeans.

They are most likely to look like the prototypical nerd

Skill

This group has a great deal of skill and can probably be considered the smartest of the categories

Great deal of knowledge about computers AND other mechanical and engineering related things

Motivation

Their goal is to gain and distribute knowledge. Least likely to be criminal.

Often fascinated with other non-computer types of hacking

"Society doesn't understand me, and technology fears me"

DEFCON

DEFCON is the original hacker conference, taking place in Las Vegas each year for the last 14 years.

The conference draws approximately 3,000-4,500 paying attendees each year.

Conference Specifics

1. **Games**: Capture the Flag, Lock pick competitions, Intrusion competitions, robot shooting competition, hacker jeopardy.
2. **Sales Area**: T-shirts, Lock Picking kits, Books, software, hardware, etc…
3. **Presentations**:
    - Hardware hacking
    - Magnetic Stipe hacking
    - Oracle Rootkits 2.0
    - Plausible Deniability Toolkit
    - Blackjacking: Owning the enterprise via the Blackberry
    - DNS Amplification attacks


WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC) W211660221)

NAME: .....MITNICK, KEVIN DAVID

AKA(S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s) 550-39-5495

Kevin Mitnick

Most famous case of hacking probably ever, although the story is not as great as many believe.

Hacked into the wrong persons, Tsutomu Shimomura, computer at the San Diego

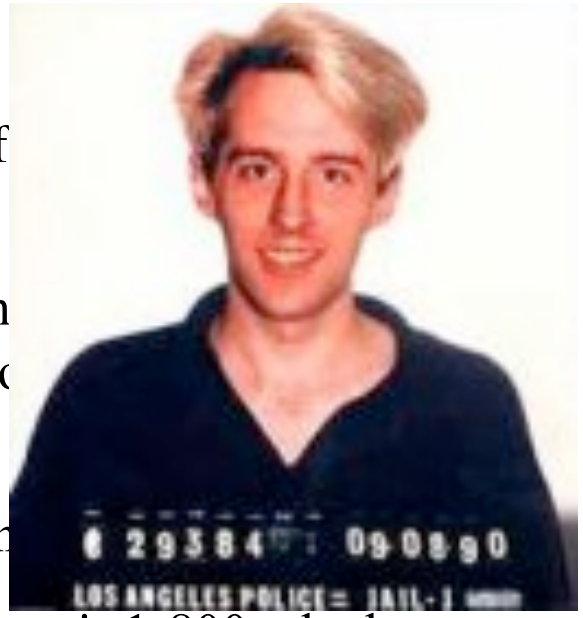
Supercomputer center.

Shimomura, then went on a mission to track him down, eventually leading the FBI to his location in Raleigh, NC.

Spent 5 years in prison and was barred from using a computer or the internet for 3 years after his release.

Now runs a successful security company and has published several books.

Kevin Poulsen



Another of the famous hackers of his day, who was known f
brought him quite a bit of noteriety.

His best-appreciated hack was a takeover of all of the teleph
Angeles radio station KIIS-FM, guaranteeing that he wo
caller, and netting him a Porsche 944 S2.

When the FBI started pursuing Poulsen, he went undergrou

When he was featured on NBC's Unsolved Mysteries, the show's 1-800 telephone lines mysteriously crashed.

He was finally arrested in April, 1991. In June 1994, Poulsen pleaded guilty to seven counts of mail, wire and computer fraud, money laundering, and obstruction of justice, and was sentenced to 51 months in prison and ordered to pay $56,000 in restitution. At the time, it was the longest sentence ever given for hacking.

He also pleaded guilty to breaking into computers and obtaining information on undercover businesses run by the FBI.

Now works as a successful journalist for CNET and Wired magazine

Robert Morris

Unleashed one of the first worms on the internet back in 1988.

Son a brilliant NSA cryptologist who learned a lot from being around his father and his fathers computers.

Had very early access to highly secret and secure networks (Bell Laboratories) where he learned his hacking skills.

When he unleashed the worm, unintentionally supposedly, it caused thousands of computers to stop working.

Credited with being the person who brought the term hacker into the public eye.

Now works for MIT as an Assistant Professor, despite unleashing the worm on MIT in 1988.

“DVD” Jon Johnasen

After posting DeCSS on the internet he was brought to a criminal trial for hacking.

The program allows users to crack the encryption program on DVD’s.

Much of the uproar which caused him to be brought to trial was from the RIAA and the MPA, which demanded that he be brought to justice.

He was found not guilty largely because he owned the DVD’s and thus was not pirating the content and he was not selling the DVD’s

The End