History & Impact of Hacking: Final Paper

From HistoryOfComputing

Contents

History & Impact of Hacking > Final Paper

Introduction by everyone

The hacker culture began in the 1960s and 1970s as an intellectual movement: exploring the unknown,

documenting the arcane, and doing what others cannot. Many hacker subcultures developed independently and in parallel at various universities throughout the United States: Stanford, MIT, CalTech, Carnegie Mellon, UC Berkeley, and many others. The completion of the ARPANET linked these campuses and they were able to share their collective experiences, their knowledge, humor and skills. Together, they formed the first hacker culture.

Many hackers began as expert programmers: programming gurus like Richard M. Stallman, founder of the Free Software Movement, and Linus Torvalds, creator of the Linux kernel. These programmers were able to found new loosely-connected organizations that would push the boundaries of accepted software engineering, and also technology. These figures serve to popularize the efforts of hacking to a society increasingly focused on computing.

In the realm of computer security, with the advent of ubiquitous networking, a distinction began to form between two groups: the so-called black hat and white hat hackers. Both maintain a connection to the haker ethic, but focus on different aspects and interpretations. The black hat culture is known for flouting authority and embracing anarchy, committing acts of mischief and malice and knowingly breaking and entering secured systems—these are the hackers most often seen in the news and popular culture. The white hats, the "ethical hackers", focus on other aspects of the hacker ethic: they seek to understand, to satiate curiosity, and to inform.

A compelling aspect of the history of hackers lies in the history of the word itself. To fully understand how and why these often mutually disparate groups happened to be called the same name, we have to examine how the computer security definition sprang from its common English definition and how it evolved to identify these different communities. While it is intractable to provide even a definite definition of "hacker" due to the constant merging and fracturing of the English language, we will at the very least, attempt to provide a chronicle of the word's new definitions from their birth to their entry into standard American English.

The Word "Hacker" by Carmelo Kintana

To use a computer science metaphor, the word “hacker” acts as a pointer to three different groups of people, the expert programmers, the black hats, and the white hats. This section will examine in detail the pointer itself. Detailed examinations of the “dereferenced” groups will take place later in the paper.

Survey of Common Definitions

We must briefly describe and define each of the three hacker groups in order to be able to flesh out the discussion properly. Many people see “hackers” as primarily referring to the people who are the most technically proficient in a certain subject. We examine a subset of this group, the "expert programmers." A separate set of “hackers” are the "black hats". The group primarily uses their skill with computers to attack computer systems and perform assorted malicious acts on their victims. This is the primary definition of hacker in the modern day. The "white hats" are the last set of "hackers." They are very similar to the black hats except they intend no malice and, indeed, may go far out of their way to prevent harm from coming to their hosts.

The groups share a few common traits between them. For example, all three groups are generally thought to possess skill superior to those of their peers. In the case of the expert programmers, this

superior skill is a defining characteristic. Indeed, if they did not possess superior skill and claimed to be a hacker, they would simply be a poseur. Additionally, the other two groups are expected to have superior skill because if they did not, they would easily be captured. Many of the perceptions of the there groups overlap as well, this will be analyzed later.

Outside of those few commonalities, the groups are very different. While the infiltration of foreign computer systems is a requirement for the black and white hats, it is irrelevant to the expert programmer. Also, the white and black hats are obviously opposites.

Etymology

The primary definition of "hacker" according to m-w.com (not counting the fruitless *"one that hacks"*) is *"a person who is inexperienced or unskilled at a particular activity."* It is remarkable that a word with this meaning would eventually pick up definition number three: *"an expert at programming and solving problems with a computer."* A quick glean of the definitions of the verb "hack" yields *"to cut or sever with repeated irregular or unskillful blows," "to clear or make by or as if by cutting away vegetation,"* and eventually *"to manage successfully."* Etymologically, the word is derived from the Old English word for "hack," "haccian". What we get from all of this is that the word originally meant *"people who chop badly"* and generalized from there.

At first glance, it may seem that our computer forefathers did not choose wisely when developing our vocabulary. To try to understand the logic behind this, we look to the very first proto-use of the word in our context. Through an in-depth search online, we find that the original source is, not surprisingly, MIT – specifically, theTech Model Railroad Club. The very first documented semi-modern use of the word "hack" is found in the club's dictionary (the dictionary's original author keeps a copy of the original dictionary on his website[1]: *"an article or project without constructive end; 2) work undertaken on bad self-advice; 3) an entropy booster; 4) to produce, or attempt to produce, a hack (3)."*

We see here the missing link between old and new definitions. We can conjecture the missing details for ourselves: To the ancients, "hack" meant to chop badly; it then aquired the meaning of doing something repetitive badly; MIT TMRC then defines it as doing something railroad-y and useless; it then becomes doing something technical and useless.At this point, hackers are those who do something technical for no reason, in other words, for fun. From here, it is a small jump to expert technical person. Thus, this is the first documented reference for our "expert programmer" definition (programmer being used loosely in this case).

Evolution

Having revealed the birth of the modern definition of hacker, we have to examine how the word moved from obscure model railroad jargon to mainstream American English. To do this, Professor Maurer suggested performing an experiment to trace the evolution of the word in a LEXIS/NEXIS search.

References for "hacker" were for cab drivers and golf until July 2, 1981 when the Canadian newspaper Globe and Mail reported on a San Francisco-based gang known as the System Hackers. The article[2] that: *"The illicit activities of the gang, and other 'phreaks' and 'hackers' as they are known, have added a new item to North America's crowded police files: juvenile computer criminals."* This is obviously also the first mainstream reference for the black hat group of hackers according to LEXIS/NEXIS. The first news transcript that contained the word was on December 4, 1984 from Ted Koppel on ABC's World News Tonight. He said, *"There've been a lot of stories recently about computer hackers, high tech experts who use*

their personal computers to break into big computer systems." This is clearly another reference to black hats.

However, upon further web searching, particularly Google News Archive Search, we came upon a Time Magazine article[3] from September 5, 1977. It read: *"Some 500 retail outlets have opened in the past couple of years to sell and service microcomputers—and serve as hangouts for the growing legions of home-computer nuts, or "hackers," as they call themselves."* This is the first mainstream reference for the "expert programmer" definition. However, while the article (which was about the popularity of low-cost microcomputers) mentions that the users called themselves hackers, the article itself preferred to use the terms "nuts" and "addicts." It is then doubtful that this article helped spur usage of the term in the mainstream.On a side note, it is surprising that LEXIS/NEXIS did not find this source but Google did.

Further searching found the first documented use in journalism. MIT's school newspaper, "The Tech," featured an article in its November 20, 1963 issue entitled *"Services Curtailed: Telephone Hackers Active[4]."* The article describes what would later be known as phreaking and the consequences for the university.

A search of the USENET archives found the first documented use of the word hacker. Kenneth Peter, alias G. Gandalf, is quoted as saying[5] on May 6, 1981: *"The commentary to the Hacker Papers (Psychology Today, Aug 80), Weizenbaum (1976), and others observe that many people appear to use computer interactions as a substitute for human interactions."* The post was rebutting a statement about the large number of gays in computer science. "The Hacker Papers" to which the post refers, is claimed to be a BBS thread regarding the overuse of computers and which was then annotated by a psychologist. We could find no reliable original copy of The Hacker Papers. The second "hacker" post, timestamped on May 10, 1981 and written by Jonathan Alan Solomon, is the first on USENET to mention hackers that is not a reference to a title: *"I tried that in my Fraternity house, I started using the 'hacker buzz words' around all the people (those like Foo, bletch, barf) but also some of the TOPS-10 system calls (exit, init.)and machine instructions (skipa, lsh)."*

No reference could be found that referred to hackers as exclusively the white hats group.

Perceptions

Having established the history of the word hacker to the present day, we will lastly examine in detail the perceptions and connotations that the word has for people today. To provide a complete picture of different groups' perceptions of the word, we need to not only analyze the views of the public toward the word "hacker," but also the views of each individual group towards the word "hacker." Keep in mind that this section is not an analysis of the perceptions of the individual groups, only the connotations of the word.

Public Perceptions

To mainstream America, a "hacker" is a black hat. Since the mainstream adoption of the word in the early 1980s, the word hacker was used to refer to black hats to what seems like the near exclusion of the other two definitions. As shown earlier, the word entered the mainstream in reference to computer vandals and this is the definition it has kept to this day. Its original use as an expert programmer has cropped up on occasion, notably, in the movie Jurassic Park, released in 1993. When Lex (the computer expert) tells her brother she is a hacker, her brother responds, *"That's what I said!You're a nerd!They don't call you people hackers anymore – they call you people nerds!"* This is clearly not a reference to a black hat.

Insider Perceptions

Unfortunately, this general perception by the mainstream that a "hacker" is a black hat has had negative consequences for the other two groups. Some of the expert group (who were the original users of the word) choose to no longer use the term due to the negative connotations, preferring instead other terms such as "geek" or "guru," depending on context. Black hats generally use the term hacker and it is not seen as a word to be avoided. White hats prefer not to use the word hacker, as they wish to distance themselves as much as possible from black hats, preferring to use the term "white hat" itself.

Even within the smaller technology community, the word hacker generally means black hat[6]. There is a significant following who strongly believe that the word hacker should exclusively mean expert programmer and prefer that the original MIT jargon term for black hat, cracker, be used instead.

To those outside this group, the word cracker is oftentimes met with derision and a flame war will occasionally ensue[7]. The proponents of "cracker" argue that the community must strive to keep the word's definition as close to its original meaning as possible. They point out that the word is heavily overloaded and the lore of its original definition may be lost. The detractors of "cracker" argue that those who use the word are out of touch and simply refuse to accept what has already been de facto settled, that the word hacker means black hat.

This section will conclude with a brief summary of how each group has contributed to the definition of hacker. The original group of experts, of course, coined the phrase and lent it its original meaning. Black hats, many of whom were experts, used the word to describe themselves, of using it as part of their "hacker gang" name. The mainstream media seized upon this and it became the widely and nearly universally accepted definition. White hats have not made any attempt to modify the definition of the word, instead clearly delineating themselves from their black hat counterparts by promoting terms such as "white hat" and "black hat."

Timeline of the word "Hack"

DATE	EVENT
circa A.D. 500	Old English word for hack, *haccian*, is used.
October 14, 1066	The Battle of Hastings is won. With the arrival of the Norman conquerors, Old English transforms into Middle English.*Haccian* becomes *hakken*.
circa A.D. 1470	The introduction of the printing press standardizes the English language. Middle English becomes Modern English. *Hakken* becomes *hack*.
circa June 1959	Peter R. Samson of the Tech Model Railroad Club of MIT publishes "AN ABRIDGED DICTIONARY of the TMRC

	LANGUAGE." It contains the first verifiable modern source of the word hacker.
November 20, 1963	MIT's newspaper, The Tech, publishes the first documented use of hacker in journalism.
September 5, 1977	Time Magazine publishes the first documented use of "hacker" in the mainstream press.
August 1, 1980	Psychology Today publishes "The Hacker Papers."
May 6, 1981	Possibly the first surviving, documented USENET post of the word hacker.
July 2, 1981	The first documented use in a newspaper of the word hacker.
December 4, 1984	The word hacker is documented to be spoken for the first time on television, by Ted Koppel.

[1] http://www.gricer.com/tmrc/dictionary1959.html

[2] http://web.lexisnexis.com/universe/document?_m=ead9b293d0bf69d7bf09ebedb13d6755&_docnu

[3] http://www.time.com/time/magazine/article/0,9171,915391,00.html

[4] http://www-tech.mit.edu/archives/VOL_083/TECH_V083_S0315_P001.pdf

[5] http://www.cs.rutgers.edu/~cwm/NetStuff/Human-Nets/Volume3.html

[6] http://it.slashdot.org/comments.pl?sid=196688&cid=16116872

[7] http://slashdot.org/comments.pl?sid=147501&cid=12358213

Expert Programmer by Vikas Rajvanshy

Hacker as an expert programmer

As the reader will be aware of by now, the term hacker is overloaded. One common use of the word is to refer to individuals who are experts in a technology field who push the technology beyond what others perceive is possible.

Impact on society

Hackers in this context have had a very measurable impact on society. If we treat the term hacker to refer to a person that pushes technology beyond perceived norms at the time, we can see several fields in computing in which they have made a measurable impact.

- Personal computing machines - Steve Wozniak is almost universally accredited with bringing the affordable PC to the masses. Whilst the precursors of the technology were already developed at PARC, it took a hacker with detailed knowledge of hardware components to meld together a PC from disparate parts at an affordable price.
- Gaming - Hackers have been pushing the limits of gaming for decades. Probably the most famous hacker in this arena is John Carmack. Carmack pioneered several technologies to push graphical capabilities of the PC beyond what was conventionally possible.
- Internet
  - Infrastructure - Tim Berners-Lee inventor of the World Wide Web.
  - Web 2.0 - AJAX the foundation of web 2.0 is often regarded as a huge hack by professional software developers. Often the constructs will bend the rules to work arround limitations in the infrastructure.
- Open Source - Linus Torvalds himself is often regarded as a hacker.

The stereotypical view of a hacker is simply an expert programmer that lacks engineering discipline and the focus required for large team projects. However most of the innovations listed above require a sustained ammount of effort.

Famous hackers

Some people might argue that based on impact, could we not say any successful technologist is a hacker? To test this and to be able to be able to rank famous hackers quantatively an experiment was conducted. The methodology was as follows:

- A base list of hackers was obtained from the Wikipedia entry on hackers.
- For each entry in this base list, two Google searches were done. The first one contained the hackers name. The second search contained the hackers name as well as the term hacker. The number of matches for each search were recorded.
- The results were analysed to see the relative number of hits, as well as the rate at which a particular hackers name appeared with the term hacker.
- These were compared against well known people in the technology industry.

Hacker	Hits on Google with term 'hacker'	Hits on Google	Hacker quotient	Relative popularity
Tim Berners-Lee	271,000	1,130,000	0.24	0.57
Dan Bernstein	14,800	93,100	0.16	0.05
John Carmack	74700	497,000	0.15	0.25
Shawn Fanning	44,200	362000	0.12	0.18
Bill Gosper	888	15800	0.06	0.01
Richard Greenblatt	877	23000	0.04	0.01
Grace Hopper	29600	245,000	0.12	0.12
Bill Joy	51,100	519,000	0.10	0.26
Donald Knuth	73,900	425,000	0.17	0.21
John McCarthy	62,400	839,000	0.07	0.42
Rob Pike	36,000	188,000	0.19	0.09
Guido van Rossum	93,900	971,000	0.10	0.49
Randal Schwartz	29,200	118,000	0.25	0.06
Richard Stallman	547,000	1,360,000	0.40	0.68
Bjarne Stroustrup	57,700	576,000	0.10	0.29
Theo de Raadt	61,300	383,000	0.16	0.19
Michael Tiemann	28,500	110,000	0.26	0.06
Linus Torvalds	1,090,000	1,990,000	0.55	1.00
Larry Wall	277000	1,150,000	0.24	0.58
Steve Wozniak	201,000	1,190,000	0.17	0.60
Wietse Venema	53,400	593,000	0.09	0.30
Rasmus Lerdorf	62,400	507,000	0.12	0.25

While there are flaws with this methodology, it does provide some interesting insight, the relative popularity is an indicator of the relative interest on the Internet. The hacker quotient is an indicator for how many people consider the person to be a hacker.

Comparing hacker quotients to other well known successful technology personalities, Bill Gates shows up with a hacker quotient of 0.08, Michael Dell shows up with 0.05. This is definately towards the bottom of all the hackers listed above. It would seem that having impact by itself is not enough to be considered a hacker.

A very interesting result is that both the top two hackers in terms of popularity and hacker quotient are strongly affiliated with the open source movement. Richard Stallman founded both the Free Software Movement and the Free Software Foundation. Linus Torvalds initiated development of the Linux kernel. Another interesting insight is that the list is predominantly populated by software hackers, the only two hardware hackers to make the list are Steve Wozniak and Richard Greenblatt.

Where did all the hardware hackers go?

As previously noted, in todays computing culture hackers seem to be focused primarily in the software arena. Looking at the major hardware hackers, one trend seems to stand out, most of them did the work that made them famous in the 1960's and 1970's. After this point there is a sharp dropoff in superstar hardware hackers. There are several plausible explanations for this:

- The barriers to entry for building computing machines were growing rapidly as economies of scale became more important.
- Software was a largely underdeveloped field that was only beginning to realize it's full potential.
- Hardware had become complex enough that a single individual could not make a measurable impact.

Likely it was a combination of these factors that led to a decline in the innovations that hackers were making in the hardware arena.

Why are the top hackers today affiliated with Open Source?

Looking at the top hackers based on the previous section, it should be clearly evident that many are strongly affiliated with the open source movement. After looking through the list and scrutinizing it in more detail, the open source connection starts to become stronger.

A prime example of a prominent hacker having strong open source leanings is how Tim Berners-Lee made his idea about the World Wide Web available freely [1]. While not directly contributing code to an open source project, he laid the foundations for what was arguably to become one of the great revolutions in computing. Another hacker, John Carmack, a very prominent video game designer is probably the most vocal advocate of open source. He also strongly opinionated with regards to patents.

John Carmack[2]: *I'm proud that there is "a relative dearth of patent applications for the video game industry, especially considering how technology-dependent the video game industry is, and given its size in terms of annual sales."*

Before issuing a condemnation, I try hard to think about it from their point of view -- the laws of the land set the rules of the game, and lawyers are deeply confused at why some of us aren't using all the tools that the game gives us.

Patents are usually discussed in the context of someone "stealing" an idea from the long suffering lone inventor that devoted his life to creating this one brilliant idea, blah blah blah.

But in the majority of cases in software, patents effect independent invention. Get a dozen sharp programmers together, give them all a hard problem to work on, and a bunch of them will come up with solutions that would probably be patentable, and be similar enough that the first programmer to file the patent could sue the others for patent infringement.

Why should society reward that? What benefit does it bring? It doesn't help bring more, better, or cheaper products to market. Those all come from competition, not arbitrary monopolies. The programmer that filed the patent didn't work any harder because a patent might be available, solving the problem was his job and he had to do it anyway. Getting a patent is uncorrelated to any positive attributes, and just serves to allow either money or wasted effort to be extorted from generally unsuspecting and innocent people or companies.

Yes, it is a legal tool that may help you against your competitors, but I'll have no part of it. Its basically mugging someone.

I could waste hours going on about this. I really need to just write a position paper some day that I can cut and paste when this topic comes up.

John Carmack

The obvious question arises, why do hackers tend to have open source leanings? There are many possible explanations, and there is likely no single explanation that fits every individual. Analyzing the open letter by John Carmack above, it would not be unreasonable to assume that his motivator is not simply profit, as he clearly states that patents will help against your competitors, however he will have no part of it. Looking at other hackers, the theme emerges again, a large majority of these hackers are not solely motivated by monetary rewards. Interestingly the cause and effect might be reversed, probably a more accurate statement would be that open source developers are more likely to be hackers, rather than vica versa. The most likely reason for this is that the innovations that hackers make are not neccessarily the best decisions to maximize economic self interest, thus there needs to be another motivator besides greed.

[1] http://www.w3.org/Consortium/Patent-Policy-20040205/

[2] http://slashdot.org/comments.pl?sid=151312&cid=12701745

What is the role of hackers in corporations?

If hackers require motivators besides profit, is there any role for them in the modern corporation? A lot of the most prominent hackers discussed so far are opposed to software patents and copyright, however their primary motivator is to push the state of the art in terms of technology. As most people know, certain fields of technology have become too capital intensive for smaller companies or groups to enter, example of this include CPU/GPU design, chip fabrication etc. Companies in such fields may be able to successfully leverage the creative power of hackers. A good example of this was how Linus Torvalds spent a period of time working at Transmeta, a commercial chip company working on cutting edge low power chips.

Some informal surveys were conducted around Microsoft, while there was evidence of Microsoft hiring both White hat and Black hat hackers, I could not find any examples of expert programmer hackers.

One possible reason is that hackers are often interested in pursuits that are not necessarily economically viable, this limits their compatibility with for profit corporations, another possibility is that Microsoft is often seen in an ideological light as opposed to the free software movement. Similar informal surveys were done on a smaller scale for several technology companies such as Amazon and Sun, and the results were similar.

Black Hat by Sandra Lemon & Hansen Liou

History

Hacker culture began as multiple independent and parallel subcultures with many traits in common; placing a high value on the freedom of information; the freedom to discover, to understand; a flouting of authority; and an eclectic sense of humor. Many trace the origins of the hacker subculture to the year 1961, when MIT first acquired the PDP-1 microcomputer. Hacker beginnings are entrenched deeply in academia; the desire to pursue knowledge unknown, to do things others cannot. The AI lab first described themselves as ‘hackers’, after their tradition of playing elaborate pranks, or ‘hacks’.

The completion of the ARPANET in the 1970's gave rise to a networked culture of hackers able to share their experiences, knowledge, jargon and humor. One of the earliest and most enduring legacies is that of the Jargon File, created in 1973 at the Stanford AI Lab (SAIL) and went through many revisions and many campuses including MIT, CMU, Yale, and many others. The Jargon File is a massive collection of hacker slang and hacker humor. Many of the references and acronyms in the Jargon File are still widely used today.

Although hacking began as an intellectual pursuit, there began a growing divide; those who hacked for the pursuit of knowledge and those who hacked with a malicious intent; to bring down systems of those they didn’t like, to steal information and secrets that were being kept. This gave rise to the black hat movement; in fact, many lawful hackers prefer that the black hats be known as crackers rather than hackers, in an attempt to distinguish themselves.

It's possible to see the growth of the black hat community simply as a byproduct of a growing society; as any society grows past a certain limit, a dark side emerges. Black hat hackers range from the mildly irritating to the genuinely malicious. There are those that simply download and use tools or exploits; these are known as 'script kiddies' and are generally frowned upon as unskilled exploiters of known bugs. There are those who 'phish' or commit acts of social engineering to seek out passwords, bank accounts, or credit card numbers by posing as members of authority. In a similar vein, there are worm authors who write self replicating programs that worm their way from computer to computer, network to network; creating an army of zombie machines, or simply disabling all machines that they encounter. And finally there is another tier; those of the elite hackers who have the skill, who make the discovery of these exploits and security lapses; these are the feared black hats, the ones who are rarely publicized but yet do all and much more than the hackers widely known.

A common tenet to all black hats that ties them together is that they knowingly commit whatever mischief or malice with the full intent of committing such acts.

Early Examples

One of the earliest examples of black hat hackers is the phone phreak who hacked for profit. The basic tool of the phone phreak was the frequency generating 'blue box' that hacked the phone system to permit the user free calls to anywhere for however long they wished. There were those who simply enjoyed the experience of phreaking; John Draper, known by his alias Captain Crunch, developed machines to seek out the limits of phone networks. There are stories of him calling the pay phone next to him and routing the call all the way across the world, from New York, to London, to Moscow, across the Pacific and back. Phone phreaks such as Mark Bernay, or "Evan Doorbell" would publish their 'phone trips' as they explored the network and connected to phones all across the United States. A sense of exploration and discovery filled many of the early generation phone phreaks; and yet, there were those involved in phreaking who created these blue box devices for use with organized crime, and would use this technology to make free phone calls for criminal purposes. The BBS era of the mid 1980s to early 1990s came, and along with it a massive spike in software piracy. Software piracy started early on; those who wanted to trade software simply did so with media, via postal mail or in person. The rise of the BBS era and networked machines allowed people to trade in much more prolific manner, especially with the use of these blue boxes for free, unlimited duration calls over which their software could be distributed.

As software companies realized their software was being traded illegally, they began implementing security measures to cope with this unauthorized distribution. These security measures gave birth to the 'cracking hacker', or 'cracker'; the black hat who broke the encryption or removed the protection so that the software was once again, free. These hackers knowingly removed commercial security measures for their personal gain, a defining characteristic of many black hats. The rise in software piracy created the warez scene; a massive network of software pirates dedicated to cracking, copying, and distributing the latest software releases.

Modern Examples & Motivations

As we look at the more recent instances of hacking, we can also analyze the motivations behind these attacks and those who execute them. The best and most detailed examples of modern hacking are those where the hackers were actually caught and tried for their crimes. Luckily for us, the FBI publishes a list of these crimes on the internet. Perhaps it's their way of hitting hackers on their playground.

Currently, the FBI's website lists over 100 computer crime cases tried in United States between 1999 and 2005. Only three were considered to be threats to public health or safety. That means most of the computer crime occurring were for financial gain or other, more complex personal reasons. Nearly one fourth of the cases were student, employees or former employees taking advantage of their internal knowledge and using it for retaliation or financial gain. Several of the accused in these cases are known members of underground hacking organizations. Their motivations must align with what society and culture generally associate with hackers: young, thrill-seekers, anti-society, bold and competitive. In most, if not all, cases, the accused is a young male. Ethnicity was not available, but most accused hackers were United States citizens.

A closer look at some of these cases can perhaps provide a better understanding of these underground hackers and their motives. In the case of United States versus Lyttle (March 11, 2005), the defendant, Robert Lyttle, 21, plead guilty to hacking into government computers and defacing government websites with material illegally obtained through his hacking. Robert Lyttle was a member of the hacking group known as "Deceptive Duo," who claimed that their intent was to inform and warn the public and the government of the vulnerabilities that existed. In fact, the group did leave their email address on the government website they defaced, insisting that they be contacted in order to assist the

government with locking down all of their systems. The meaning of the group's name coupled with the defendant's previous encounter with the law for defacing public web sites in protest of the recording industry's injunction on file-sharing Napster does provide some doubt into the innocence of his attack Surely, he must have known defacing a government website would draw attention and punishment of some form. Some would speculate that the attention and fame (bragging-rights) are more desired than the attempt to warn the government of security failings. Lyttle received four months in prison, four months of house arrest and was ordered to repay over $70,000.

Max Butler was prosecuted in 2000 for hacking into government systems, he was 28. His story is different because he was (supposedly) a white hat hacker and working with the FBI as an informant. The temptation must have been too great because he broke into thousands of government computers. On the surface, it looked as if he was simply being helpful, because he patched the flaw that allowed him in, effectively disallowing other hackers in. Unfortunately for him, while there, he created a back door so that only he could return. Conspiracy theorists would say that there is much more to this case, but we're simply interested in his motivations of hacking. While serving his 18 month prison term, Butler gave a telephone interview and attributed his actions to a combination of peer pressure and hacker pride. "I'd heard of this sort of thing all my life," said Butler. "To see all these dot-mil's scroll up the screen... there was a certain sort of thrill to it… I knew that I shouldn't have been doing what I was doing, but I had good intentions overall, and I closed this hole in thousands of systems, probably tens of thousands of system."

In United States versus Smith (May 2, 2002), David L. Smith, 34, plead guilty to knowingly spreading a computer virus with the intent to cause damage. His virus, known as Melissa, infected users through an email and infected the computer's Microsoft Outlook to send the same infectious email to the first 50 contacts. The Melissa virus spread quickly and caused over $80 million in damage and is to-date the most costly computer outbreak. His sentence of 10 years was reduced to 20 months and a $5,000 fine when he agreed to work undercover for the FBI. He has helped to track down numerous offenders, mainly through signatures and bragging quotes they leave embedded in their malicious code. The intent to take credit is apparently greater than the intent to not get caught.

Impact of Hacking on Businesses and Governments

Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customers' personal and financial data and often are targeted by their own employees, whether disgruntled or just opportunistic. Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can linger for years after the actual attack. Companies can lose consumer confidence and in many cases are held legally responsible for any loss to their customers. The cost of recovering from an attack can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc. Companies, and more recently, consumers, are investing more and more money into preventing an attack before it actually happens.

Businesses that hold stores of consumer's personal and financial data are especially taking extra steps to insure the data's safety. Microsoft's online group, MSN/Windows Live, requires that no single group store personally identifiable information without explicit consent from an internal security group. Security reviews occur frequently for groups that do store consumers' data and the security group performs its own personal security review by actually attempting to hack into the sites. Sites have actually been witheld from releasing to the web due to flaws found through this method.

Other businesses that are more limited in technical areas employ outside security experts to assist

them with their security. ScanAlert.com boasts of working with over 75,000 secure ecommerce sites, including many famous brands like FootLocker, Restoration Hardware and Sony. The ecommerce sites host a “Hacker Safe” logo, stating that the site is tested daily and is effectively preventing 99.9% of hacker crime. The ScanAlert disclaimer though appears far less confident:

> *This information is intended as a relative indication of the security efforts of this web site and its operators. While this, or any other, vulnerability testing cannot and does not guarantee security; it does show that [the eCommerce Site] meets all payment card industry guidelines for remote web server vulnerability testing to help protect your personal information from hackers. HACKER SAFE does not mean hacker proof. HACKER SAFE certification cannot and does not protect any of your data that may be shared with other servers that are not certified HACKER SAFE, such as credit card processing networks or offline data storage, nor does it protect you from other ways your data may be illegally obtained such as non-hacker ”insider” access to it. While ScanAlert makes reasonable efforts to assure its certification service is functioning properly, ScanAlert makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that ScanAlert shall be held harmless in any event.*

Businesses, in recent years, have also had to deal with a specialized and more challenging type of hacking. Social engineering is a way of defrauding a user into providing you with information not normally available to you, whether it be a password, access code or other piece of information necessary in hacking into a computer system. Similar to phishing, social engineering relies on tricking a person or group of people in order to be successful. While not normally the tactics associated with a hacker, famous hackers like Kevin Mitnick have used it in their crimes and claim it to be one of the most effective means of hacking.

Digital piracy is also seen as a form of hacking. The massive rise of content available on the internet and it's associated theft has changed the way many people and many industries view security. No longer do pirates only traffic in software; movies, music and other media are also high profile targets. This theft and uproar by content owners (music and movie industries claim to lose billions) has been so great that the United States passed a law that "criminalizes production and dissemination of technology whose primary purpose is to circumvent measures taken to protect copyright, not merely infringement of copyright itself, and heightens the penalties for copyright infringement on the Internet". The law, called the Digital Millenium Copyright Act (DMCA), specifically targets not only the group trafficking the pirated goods, but the act of removing the protections themselves. Hackers can no longer claim an 'academic' pursuit of knowledge in circumventing security techniques; the very act has been deemed a criminal offense.

Companies, especially software companies, also have to be very careful within their own employee base. Some of the most costly hacking crimes hack been due to internal employees, sometimes ex-employees, taking advantage of their access to passwords, networks and financial information. A UBS PaineWebber system administrator planted a virus on the company network in 2002 which deleted files and destroyed data, causing over $3 million in damage. The employee was apparently dissatisfied with his salary and had put tens of thousands of dollars into stocks that would only be valuable with his company’s demise. Opportunistic attacks like these are hard to avoid.

As the number of computer crimes has risen over the last few decades, so have consumer fears and with them, a large number of security companies. In the 2005 FBI Computer Crime Survey, 98% of companies surveyed used at least some form of security technology. At least 75% of the companies utilized anti-spamware software, anti-spyware software, firewalls and anti-virus software. Still, over 79% of companies surveyed were adversely affected by spyware and viruses, worms or trojans, all within the surveyed year.

In coordination with security efforts, software engineers have had to learn a great deal about hacking. The best way to avoid hacking attacks is to avoid defective code, and software companies are especially criticized on this issue. Microsoft, in particular, has been greatly scrutinized over the number of exploitations in their software. Microsoft has made a valid attempt to limit these security holes over the years, but if nothing else, has created a culture of continuously updating software to compensate for the flaws.

Web development is particularly vulnerable to hacking, especially with the rise of Web 2.0. Software engineers working on the web have to be prodigious to avoid issues like cross site scripting and sql injection, where malicious users can exploit simple holes in web sites to steal data or trick consumers. Instructions to exploitations like these are readily available on the internet, allowing everyday people to hack systems.

Other businesses have chosen to place their trust in the very hands of hackers. While many companies express fear at trusting someone who can do so much danger, other companies take advantage of their skills in hopes of avoiding attacks by more malicious hackers. Microsoft, for instance, announced at a Black Hat security conference this year that they have been working with several groups of famous, reformed hackers in attempts to prevent security holes in their upcoming and widely debated operating system. It seems like risky business to trust those who only years before were exploiting the very, but it seems to be paying off for Microsoft. But normal critics of Microsoft's lackadaisical attitude towards software have recently stepped forward to compliment Microsoft's attempts at securing Vista before its release, partly due to its relationships with hackers. Still, some critics think aligning with hackers is a dangerous game and purely a marketing attempt to convince consumers of their security efforts.

Microsoft and other companies hit by the effects of hacking are also joining forces with government agencies. The FBI started an organization called InfraGard, whose mission is to "improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures." It's basically a way of keeping communication open between the public and private sector in regards to all types of computer crime: unstructured threats (insiders, recreational hackers, and institutional hackers), structured threats (organized crime, industrial espionage and terrorists), and national security threats (intelligence agencies and information warriors). Another organization, the Computer Emergency Response Team (CERT), is available even to civilians and allows anyone to notify them of a cyber threat directly through their web site. They are a part of the Department of Homeland Security and focus more on common frauds like phishing.

Aside from preventing hacking, the government has had to pass a great deal of legislation in order to effectively deal with computer crimes. The "Computer Fraud and Abuse Act" was passed in 1988 to limit the hacking of computer systems and covers crimes like unauthorized access to national security data, unauthorized access to data within financial institutions, transmitting code that do harm whether financial or physical and even covers some forms of social engineering. The law has been amended several times, most recently with the Patriot Act which lowered the bar for violations and increased the severity of punishments for violators.

Other countries have created similar laws for themselves: Australia created Cybercrime Act of 2001, UK created the Computer Misuse Act of 1990, etc. Governments even joined forces to create the first international treaty regarding computer crime, called the Convention on Cybercrime. Over 40 nations have signed the treaty, including the United States in August of 2006. Hacking has become one of the most egregious crimes and has had far-reaching effects.

White Hat by Michael Frederick

The practice of white hat-hacking (also known as ethical hacking) has recently been the focus of much debate among computer security professionals. Many of the current group of white hats arose from the same culture that produced black hats, or are former black hats themselves. Contrasting with the person who hacks a system for personal profit, or a sense of mischievousness, a white hat does so out of a perceived ethical responsibility, or a sense of curiosity, with the intended result being an enhanced understanding of security practices and the hardening of computer systems. According to Richard Stallman, the distinction between black and white hat hackers can be characterized as "hackers who turn new ideas toward destructive, malicious ends versus hackers who turn new ideas toward positive or, at the very least, informative ends."[1]

Motivations

The "Hacker Ethic," as described by Steven Levy in his book Hackers, introduces two important principles into a discussion of computer and information security: "2. All information should be free. 3. Mistrust authority - promote decentralization."[2] What is crucial to understand about this passage is that its interpretation is key to understanding the nature of the hacker. A black hat may see the freeing of arbitrary or private information as adherence to the ethic, as well as any act that destabilizes the industry. To a white hat, this ethic will imbue a personal responsibility to distinguish the types of information that should be free from those that should not. Few hackers would agree to the idea of having all personal information freely available to any for the taking. Those that do would also support the type of anarchy that tends to brew in hacker organizations. To a white hat, the decentralization of authority does not imply anarchy, but a more democratic ideal.

Kevin Mitnick

Mitnick, once the most infamous hacker in the world, is now the owner of a security company that specializes in hacking into its clients, employing some of the techniques that Mitnick used in his previous criminal activities. While Mitnick never profited from his illegal hacking, he felt no ethical responsibility to his victims. "So, it's kind of interesting, because what other criminal activity can you ethically practice? You can't be an ethical robber. You can't be an ethical murderer. So it's kind of ironic. But it is really rewarding to know that I can take my background and skills and knowledge and really help the community."[3]

H.D. Moore

Found of the open source Metasploit project, which purports to "provide useful information to people who perform penetration testing, IDS signature development, and exploit research….The tools and information on this site are provided for legal security research and testing purposes only." Critics of the project claim that this site provides the same research and tools to the would-be malicious hackers, and that disclosure of this information is tantamount to "aiding and abetting the enemy."

History

Rising out of the black hat community

In the eyes of many, it may be difficult to discern the difference between white and black hat hacking.

To a system administrator on the inside of a corporate firewall, the motivations or ethical code of the person “attacking” their system may be irrelevant. Yet it is the ethical code that typically distinguishes the two types.

Whereas black hats are often seen as having dubious or nonexistent ethical values, white hats define themselves by their adherence to the hacker ethic, and specifically using their skills to help people, and companies defend themselves against black hats. Although, as noted in the case of Max Butler, an ethical "accounting" system may still lead a hacker to do destructive things in the name of security. Hackers, as humans, are enormously complex creatures. It would be facile to assume that hackers strictly adhere to their ethical code at all times. But in defining what a white hat is, a good definition could be "one who hacks under a set of ethical guidelines and does so for the good of individuals and society." This definition could imply that many common white hats do not deserve the title as they may be primarily motivated by earning a living at their jobs.

While there is a current trend to pigeonhole a hacker in either the white or black hat camp, this was not always the case. Many hackers consider themselves "grey hats," implying that the label is less important than the hacking. Perhaps most hackers belong in this category, since there are few unambiguously good or bad people, and a good person may commit harmful acts. Still, in general, the labels are useful.

Reformation of former black hats

As in the Kevin Mitnick case, there are many former black hat hackers who are now employed in the computer security industry. While it may be difficult to assume an ethical change in the hacker, since they are being compensated and legitimized by these companies, it no doubt reflects a change in the intended outcome of their actions.

Hacker literature

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 was 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."

Popular culture

Images of white hat hackers may be found in many movies and books. In Hollywood, the main characters in the move The Matrix start out as simple computer hackers who end up fighting for the fate of human civilization. Other movies include Hackers and Sneakers.

Impact

Society

In 2002, a group of hackers known as el8 began a campaign of cyberterrror against known white hat hackers called Project Mayhem, which has the purported goal of "[causing] worldwide physical destruction to the security industry infrastructure." This group sees the success of ethical hacking as a personal affront to their own ideals, and as a general corruption of the Hacker Ethic. From the "New Hacking Manifesto" by el8 member cr4zy c0nsuel0:

> I am a Hacker, dont try to understand me, you lost all hope of that when you crossed the line. You fail to see the lies and utter simplicity behind the computer security industry. Once, you may have shared my ideals. You fail to see the fact that security is a maintenance job. Youve given up hope for something better. You fail to see yourself as worthless, fueling an industry whose cumulative result is nothing. I dont hate you, I dont even really care about you - If you try to stop me, you will fail, because I do this out of love -- you do it for money.

This sense of betrayal is spread throughout the Project Mayhem site and literature. Whether the complaint is legitimate, and ethical hackers are more often promoting themselves and their services, the overall perception of the material is one of personal effrontery, not one based in idealogy.

Security

According to the Bureau of Labor Statistics, jobs for computer security professionals are rising "much faster than average," the highest level that the bureau measures. A growing job market would lead one to conjecture that more hackers will see this as a potential career path. From an economic perspective, there may be more to gain via a legitimate paycheck than that which arises from whatever satisfying malicious or personal curiousity, or gaining infamy in the black hat community. The other side of this issue is that in a society increasingly focused on security, there may be more to gain as a black hat.

One of the more controversial aspects of ethical hacking is the concept of disclosure. Software vendors would greatly prefer to have knowledge of potential bugs or possible exploits before it reaches the public. For the vendor, it gives them an opportunity to patch the problem before it is exploited in the wild. But many hackers in the community feel that full, public disclosure is the only method to ensure that vendors will act upon the discovery of these exploits, and release patches for all customers. The vendors counter that this allows malicious software to be created as the patches are being developed. H.D. Moore elaborates on the concept of full disclosure thusly: "Partial disclosure never works. You

just end up catering to special groups that you deem trustworthy enough to have access."

Although somewhat controversial, the hiring of former black hats as security professionals is seen as a necessary evil, since the hackers possess the skills and mindset of the people that they are employed to defend against. There is a debate over the efficacy of former black hats in a security role. While they may possess skills and information important in the attack of systems, it is not clear whether those same skills are critical in the defense of the same system. Said Paul Ducklin, chief technical officer at Sophos: "I don't know why people think if you can trot out 10 or 20 or 100 viruses, you would be great at actually producing some antivirus technology that can deal with 200,000 different bits of malware."[4]

[1] Free as in Freedom: Richard Stallman's Crusade for Free Software. Williams, Sam. 2002. (http://www.faifzilla.org/)

[2] Hackers : heroes of the computer revolution. Levy, Steven. Anchor Press/Doubleday, 1984.

[3] The mind of HD Moore. Roberts, Paul F. Infoworld, July 31, 2006 (http://www.infoworld.com/article/06/07/31/31NMmain_1.html)

[4] Do former black hats make good hires? Yeo, Vivian. ZDNet Asia, September 26, 2006 (http://www.zdnetasia.com/insight/security/0,39044829,61955207,00.htm)

Conclusion by everyone

From lofty beginnings as expert programmers and curious intellectuals, the hacker mentality evolved over time into a multifarious world view. Hacking is seen in programming, and in the legal, semi-legal, and illegal activities of many white, grey, and black hat hackers. All seem to adhere to different aspects of the Hacker Ethic.

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.

In the security realm, we see more and more activity: spyware, viruses, spam. But as the number of malicious black hats increases, we can expect a corresponding increase of security jobs and white hats. We expect more and more high-profile attacks on public targets, and tighter controls via legislature.

The future of the word "hacker" is unlikely to be as varied as its past. Since the word has entered the mainstream and many members of the hacker community are willing to let the eternal "hacker vs. cracker" flame war die, we can predict that "black hat" will be its primary definition as we move into the future. This prediction, of course, makes the tenuous assumption that no new definitions develop. Given that the current definition has disseminated with such great speed and over the violent objections of the original hacker community, it is certainly likely that with the endorsement of the journalism community and the wider English-speaking world, this nascent definition of hacker may

usurp the old one.

References

http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_thr Symantec Internet Security Threat Report, Trends for January 06–June 06, Volume X. Sep. 2006.

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

http://www.wired.com/news/politics/0,1283,44007,00.html A 'White Hat' Goes to Jail. Michelle Delio. Wired News. May 22, 2001.

http://www.eweek.com/article2/0,1895,1999070,00.asp Microsoft Takes LSD to Test Vista Security. eWeek.com. Ryan Nairaine. Aug. 4, 2006.

http://www.eweek.com/article2/0,1895,1998034,00.asp FBI: Hackers Must Help Fight Web Mob. eWeek.com. Ryan Nairaine. Aug. 2, 2006.

http://www.time.com/time/digital/digital50/10.html John Carmack in Time Digital Archive.

http://www.theregister.co.uk/2001/07/05/max_vision_begins_18month_term/ Max Vision begins 18-month term, Joins growing hacker population in stir. Kevin Poulson. The Register. July 5, 2001.

http://en.wikipedia.org/wiki/Social_engineering_(computer_security) Social Engineering. Wikipedia.org.

http://en.wikipedia.org/wiki/DMCA DMCA. Wikipedia.org

http://jargon-file.org/archive/ The Jargon File Archive

http://www.mithral.com/~beberg/manifesto.html The Hacker Manifesto

http://www.infragard.net/

http://www.us-cert.gov/

http://en.wikipedia.org/wiki/Convention_on_Cybercrime

http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html A convicted hacker debunks some myths. CNN.com. October 13, 2005

http://web.lexis-nexis.com/universe/document?_m=7aac67aa4fca66a2be06b803c9bfecef&_docnun SURVEY - CORPORATE SECURITY: The black arts of 'white hat' hackers.

http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/in Why Attacking Systems Is a Good Idea. Iván Arce, Gary McGraw. IEEE Security & Privacy. July/August 2004.

http://manifest.net.ru/manifest_en.html Manifest

http://www.wired.com/news/culture/0,1284,54400,00.html White-Hat Hate Crimes on the Rise. Brian McWilliams. Wired News. Aug, 13, 2002.

http://el8.ru/texts/manifesto.txt New Hacking Manifesto. cr4zy c0nsuel0.