WIKIPEDIA

Hacker

A computer **hacker** is a computer expert who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. Though the term *hacker* has become associated in popular culture with a *security hacker* – someone who utilizes their technical know-how of bugs or exploits to break into computer systems and access data which would otherwise be unavailable to them – hacking can also be utilized by legitimate figures in legal situations. For example, law enforcement agencies sometimes use hacking techniques in order to collect evidence on criminals and other malicious actors. This could include using anonymity tools (such as a VPN, or the dark web) to mask their identities online, posing as criminals themselves.[1][2] Likewise, covert world agencies can employ hacking techniques in the legal conduct of their work. Oppositely, hacking and cyber-attacks are used extra- and illegally by law enforcement and security agencies (conducting warrantless activities), and employed by State actors as a weapon of both legal and illegal warfare.

Contents

Definitions

General definition

Reflecting the two types of hackers, there are two definitions of the word "hacker":

1. Originally, hacker simply meant advanced computer technology enthusiast (both hardware and software) and adherent of programming subculture; see hacker culture.[3]
2. Someone who is able to subvert computer security. If doing so for malicious purposes, the person can also be called a cracker.[4]

Today, mainstream usage of "hacker" mostly refers to computer criminals, due to the mass media usage of the word since the 1990s.[5] This includes what hacker slang calls "script kiddies", people breaking into computers using programs written by others, with very little knowledge about the way they work. This usage has become so predominant that the general public is largely unaware that different meanings exist.[6] While the self-designation of hobbyists as hackers is generally acknowledged and accepted by computer security hackers, people from the programming subculture consider the computer intrusion related usage incorrect, and emphasize the difference between the two by calling security breakers "crackers" (analogous to a safecracker).

The controversy is usually based on the assertion that the term originally meant someone messing about with something in a positive sense, that is, using playful cleverness to achieve a goal. But then, it is supposed, the meaning of the term shifted over the decades and came to refer to computer criminals.[7]

As the security-related usage has spread more widely, the original meaning has become less known. In popular usage and in the media, "computer intruders" or "computer criminals" is the exclusive meaning of the word today. (For example, "An Internet 'hacker' broke through state government security systems in March.") In the computer enthusiast (Hacker Culture) community, the primary meaning is a complimentary description for a particularly brilliant programmer or technical expert. (For example, "Linus Torvalds, the creator of Linux, is considered by some to be a hacker.") A large segment of the technical community insist the latter is the "correct" usage of the word (see the Jargon File definition below).

Representation in mainstream media

The mainstream media's current usage of the term may be traced back to the early 1980s. When the term, previously used only among computer enthusiasts, was introduced to wider society by the mainstream media in 1983,[8] even those in the computer community referred to computer intrusion as "hacking", although not as the exclusive definition of the word. In reaction to the increasing media use of the term exclusively with the criminal connotation, the computer community began to differentiate their terminology. Alternative terms such as "cracker" were coined in an effort to maintain the distinction between "hackers" within the legitimate programmer community and those performing computer break-ins. Further terms such as "black hat", "white hat" and "gray hat" developed when laws against breaking into computers came into effect, to distinguish criminal activities from those activities which were legal.

Representation in network news

However, network news use of the term consistently pertained primarily to the criminal activities, despite the attempt by the technical community to preserve and distinguish the original meaning, so today the mainstream media and general public continue to describe computer criminals, with all levels of technical sophistication, as "hackers" and do not generally make use of the word in any of its non-criminal connotations. Members of the media sometimes seem unaware of the distinction, grouping legitimate "hackers" such as Linus Torvalds and Steve Wozniak along with criminal "crackers".[9]

As a result, the definition is still the subject of heated controversy. The wider dominance of the pejorative connotation is resented by many who object to the term being taken from their cultural jargon and used negatively,[10] including those who have historically preferred to self-identify as hackers. Many advocate using the more recent and nuanced alternate terms when describing criminals and others who negatively take advantage of security flaws in software and hardware. Others prefer to follow common popular usage, arguing that the positive form is confusing and unlikely to become widespread in the general public. A minority still use the term in both senses despite the controversy, leaving context to clarify (or leave ambiguous) which meaning is intended.

However, because the positive definition of hacker was widely used as the predominant form for many years before the negative definition was popularized, "hacker" can therefore be seen as a shibboleth, identifying those who use the technically-oriented sense (as opposed to the exclusively intrusion-oriented sense) as members of the computing community. On the other hand, due to the variety of industries software designers may find themselves in, many prefer not to be referred to as hackers because the word holds a negative denotation in many of those industries.

A possible middle ground position has been suggested, based on the observation that "hacking" describes a collection of skills and tools which are used by hackers of both descriptions for differing reasons. The analogy is made to locksmithing, specifically picking locks, which is a skill which can be used for good or evil. The primary weakness of this analogy is the inclusion of script kiddies in the popular usage of "hacker," despite their lack of an underlying skill and knowledge base.

Sometimes, "hacker" is simply used synonymously with "geek": "A true hacker is not a group person. He's a person who loves to stay up all night, he and the machine in a love-hate relationship... They're kids who tended to be brilliant but not very interested in conventional goals It's a term of derision and also the ultimate compliment."[11]

Fred Shapiro thinks that "the common theory that 'hacker' originally was a benign term and the malicious connotations of the word were a later perversion is untrue." He found that the malicious connotations were already present at MIT in 1963 (quoting *The Tech*, an MIT student newspaper), and at that time referred to unauthorized users of the telephone network,[12][13] that is, the phreaker movement that developed into the computer security hacker subculture of today.

Types

Hacker culture

Hacker culture is an idea derived from a community of enthusiast computer programmers and systems designers in the 1960s around the Massachusetts Institute of Technology's (MIT's) Tech Model Railroad Club (TMRC)[14] and the MIT Artificial Intelligence Laboratory.[15] The concept expanded to the hobbyist home computing community, focusing on hardware in the late 1970s (e.g. the Homebrew Computer Club)[16] and on software (video games,[17] software cracking, the demoscene) in the 1980s/1990s. Later, this would go on to encompass many new definitions such as art, and life hacking.

Security related hacking

Security hackers are people involved with circumvention of computer security. Among security hackers, there are several types, including:

White hat hacker

White hats are hackers who work to keep data safe from other hackers by finding system vulnerabilities that can be mitigated. White hats are usually employed by the target system's owner and are typically paid (sometimes quite well) for their work. Their work is not illegal because it is done with the system owner's consent.

Black hat hacker

Black hats or crackers are hackers with malicious intentions. They often steal, exploit, and sell data, and are usually motivated by personal gain. Their work is usually illegal. A cracker is like a black hat hacker,[18] but is specifically someone who is very skilled and tries via hacking to make profits or to benefit, not just to vandalize. Crackers find exploits for system vulnerabilities and often use them to their advantage by either selling the fix to the system owner or selling the exploit to other black hat hackers, who in turn use it to steal information or gain royalties.

Grey hat hacker

Grey hats include those who hack for fun or to troll. They may both fix and exploit vulnerabilities, but usually not for financial gain. Even if not malicious, their work can still be illegal, if done without the target system owner's consent, and grey hats are usually associated with black hat hackers.

Motives

Four primary motives have been proposed as possibilities for why hackers attempt to break into computers and networks. First, there is a criminal financial gain to be had when hacking systems with the specific purpose of stealing credit card numbers or manipulating banking systems. Second, many hackers thrive off of increasing their reputation within the hacker subculture and will leave their handles on websites they defaced or leave some other evidence as proof that they were involved in a specific hack. Third, corporate espionage allows companies to acquire information on products or services that can be stolen or used as leverage within the marketplace. And fourth, state-sponsored attacks provide nation states with both wartime and intelligence collection options conducted on, in, or through cyberspace.[19]

Overlaps and differences

The main basic difference between programmer subculture and computer security hacker is their mostly separate historical origin and development. However, the *Jargon File* reports that considerable overlap existed for the early phreaking at the beginning of the 1970s. An article from MIT's student paper *The Tech* used the term hacker in this context already in 1963 in its pejorative meaning for someone messing with the phone system.[12] The overlap quickly started to break when people joined in the activity who did it in a less responsible way.[20] This was the case after the publication of an article exposing the activities of Draper and Engressia.

According to Raymond, hackers from the programmer subculture usually work openly and use their real name, while computer security hackers prefer secretive groups and identity-concealing aliases.[21] Also, their activities in practice are largely distinct. The former focus on creating new and improving existing infrastructure (especially the software environment they work with), while the latter primarily and strongly emphasize the general act of circumvention of security measures, with the effective use of the knowledge (which can be to report and help fixing the security bugs, or exploitation reasons) being only rather secondary. The most visible difference in these views was in the design of the MIT hackers' Incompatible Timesharing System, which deliberately did not have any security measures.

There are some subtle overlaps, however, since basic knowledge about computer security is also common within the programmer subculture of hackers. For example, Ken Thompson noted during his 1983 Turing Award lecture that it is possible to add code to the UNIX "login" command that would accept either the intended encrypted password or a particular known password, allowing a backdoor into the system with the latter password. He named his invention the "Trojan horse". Furthermore, Thompson argued, the C compiler itself could be modified to automatically generate the rogue code, to make detecting the modification even harder. Because the compiler is itself a program generated from a compiler, the Trojan horse could also be automatically installed in a new compiler program, without any detectable modification to the source of the new compiler. However, Thompson disassociated himself strictly from the computer security hackers: "I would like to criticize the press in its handling of the 'hackers,' the 414 gang, the Dalton gang, etc. The acts performed by these kids are vandalism at best and probably trespass and theft at worst. ... I have watched kids testifying before Congress. It is clear that they are completely unaware of the seriousness of their acts."[22]

The programmer subculture of hackers sees secondary circumvention of security mechanisms as legitimate if it is done to get practical barriers out of the way for doing actual work. In special forms, that can even be an expression of playful cleverness.[23] However, the systematic and primary engagement in such activities is not one of the actual interests of the programmer subculture of hackers and it does not have significance in its actual activities, either.[21] A further difference is that, historically, members of the programmer subculture of hackers were working at academic institutions and used the computing environment there. In contrast, the prototypical computer security hacker had access exclusively to a home computer and a modem. However, since the mid-1990s, with home computers that could run Unix-like operating systems and with inexpensive internet home access being available for the first time, many people from outside of the academic world started to take part in the programmer subculture of hacking.

Since the mid-1980s, there are some overlaps in ideas and members with the computer security hacking community. The most prominent case is Robert T. Morris, who was a user of MIT-AI, yet wrote the Morris worm. The *Jargon File* hence calls him "a true hacker who blundered".[24] Nevertheless, members of the programmer subculture have a tendency to look down on and disassociate from these overlaps. They commonly refer disparagingly to people in the computer security subculture as crackers and refuse to accept any definition of hacker that encompasses such activities. The computer security hacking subculture, on the other hand, tends not to distinguish between the two subcultures as harshly, acknowledging that they have much in common including many members, political and social goals, and a love of learning about technology. They restrict the use of the term cracker to their categories of script kiddies and black hat hackers instead.

All three subcultures have relations to hardware modifications. In the early days of network hacking, phreaks were building blue boxes and various variants. The programmer subculture of hackers has stories about several hardware hacks in its folklore, such as a mysterious "magic" switch attached to a PDP-10 computer in MIT's AI lab that, when switched off, crashed the computer.[25] The early hobbyist hackers built their home computers themselves from construction kits. However, all these activities have died out during the 1980s when the phone network switched to digitally controlled switchboards, causing network hacking to shift to dialing remote computers with modems when pre-assembled inexpensive home computers were available and when academic institutions started to give individual mass-produced workstation computers to scientists instead of using a central timesharing system. The only kind of widespread hardware modification nowadays is case modding.

An encounter of the programmer and the computer security hacker subculture occurred at the end of the 1980s, when a group of computer security hackers, sympathizing with the Chaos Computer Club (which disclaimed any knowledge in these activities), broke into computers of American military organizations and academic institutions. They sold data from these machines to the Soviet secret service, one of them in order to fund his drug addiction. The case was solved when Clifford Stoll, a scientist working as a system administrator, found ways to log the attacks and to trace them back (with the help of many others). *23*, a German film adaption with fictional elements, shows the events from the attackers' perspective. Stoll described the case in his book *The Cuckoo's Egg* and in the TV documentary *The KGB, the Computer, and Me* from the other perspective. According to Eric S. Raymond, it "nicely illustrates the difference between 'hacker' and 'cracker'. Stoll's portrait of himself, his lady Martha, and his friends at Berkeley and on the Internet paints a marvelously vivid picture of how hackers and the people around them like to live and how they think."[26]

See also

- Script kiddie, an unskilled computer security attacker

References

1. Ghappour, Ahmed (2017-01-01). "Tallinn, Hacking, and Customary International Law" (https://scholarship.law.bu.edu/faculty_scholarship/206). *AJIL Unbound*. **111**: 224–228. doi:10.1017/aju.2017.59 (https://doi.org/10.1017%2Faju.2017.59). S2CID 158071009 (https://api.semanticscholar.org/CorpusID:158071009).
2. Ghappour, Ahmed (2017-04-01). "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web" (https://scholarship.law.bu.edu/faculty_scholarship/204). *Stanford Law Review*. **69** (4): 1075.
3. *Hackers: Heroes of the Computer Revolution*. 1984.
4. "Internet Users' Glossary" (https://web.archive.org/web/20160605204821/https://tools.ietf.org/html/rfc1983). Archived from the original (https://tools.ietf.org/html/rfc1983) on 2016-06-05.RFC 1983
5. Skillings, Jon (27 May 2020). "In '95, these people defined tech: Gates, Bezos, Mitnick and more" (https://web.archive.org/web/20200528205149/https://www.cnet.com/news/in-95-these-people-defined-tech-gates-gosling-bezos-mitnick-and-more/). *CNET*. Archived from the original (https://www.cnet.com/news/in-95-these-people-defined-tech-gates-gosling-bezos-mitnick-and-more/) on 28 May 2020. Retrieved 28 May 2020. "The term "hacker" started out with a benign definition: It described computer programmers who were especially adept at solving technical problems. By the mid-1990s, however, it was widely used to refer to those who turned their skills toward breaking into computers, whether for mild mischief or criminal gain. Which brings us to Kevin Mitnick."
6. Yagoda, Ben. "A Short History of "Hack" " (http://www.newyorker.com/tech/elements/a-short-history-of-hack). *The New Yorker*. Retrieved November 3, 2015.
7. "Internet Users' Glossary" (https://web.archive.org/web/20160516153012/https://tools.ietf.org/html/rfc1392). Archived from the original (https://tools.ietf.org/html/rfc1392) on 2016-05-16.RFC 1392
8. Deffree, Suzanne (2019-09-05). "EDN - 'Hacker' is used by mainstream media, September 5, 1983" (https://www.edn.com/hacker-is-used-by-mainstream-media-september-5-1983/). *EDN*. Retrieved 2020-09-07.
9. DuBois, Shelley. "A who's who of hackers" (https://web.archive.org/web/20110619062251/http://tech.fortune.cnn.com/2011/06/16/a-whos-who-of-hackers/). *Reporter*. Fortune Magazine. Archived from the original (http://tech.fortune.cnn.com/2011/06/16/a-whos-who-of-hackers/) on June 19, 2011. Retrieved 19 June 2011.
10. "TMRC site" (https://web.archive.org/web/20060503072049/http://tmrc.mit.edu/hackers-ref.html). Archived from the original (http://tmrc.mit.edu/hackers-ref.html) on 2006-05-03.
11. Alan Kay quoted in Stewart Brand, "S P A C E W A R: Fanatic Life and Symbolic Death Among the Computer Bums:" In *Rolling Stone* (1972)
12. Fred Shapiro: Antedating of "Hacker" (http://listserv.linguistlist.org/cgi-bin/wa?A2=ind0306B&L=ads-l&P=R5831&m=24290) Archived (https://web.archive.org/web/20071025200829/http://listserv.linguistlist.org/cgi-bin/wa?A2=ind0306B&L=ads-l&P=R5831&m=24290) 2007-10-25 at the Wayback Machine. *American Dialect Society Mailing List* (13. June 2003)
13. "The Origin of "Hacker" " (https://imranontech.com/2008/04/01/the-origin-of-hacker/). April 1, 2008.

14. London, Jay (6 April 2015). "Happy 60th Birthday to the Word "Hack" " (https://web.archive.org/web/20160507193534/https://slice.mit.edu/2015/04/06/happy-birthday-hack/). Archived from the original (https://slice.mit.edu/2015/04/06/happy-birthday-hack/) on 7 May 2016. Retrieved 16 December 2016.
15. Raymond, Eric (25 August 2000). "The Early Hackers" (http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/ar01s02.html). *A Brief History of Hackerdom*. Thyrsus Enterprises. Retrieved 6 December 2008.
16. Levy, part 2
17. Levy, part 3
18. "What are crackers and hackers? | Security News" (https://web.archive.org/web/20110515044743/http://www.pctools.com/security-news/crackers-and-hackers/). *www.pctools.com*. Archived from the original (http://www.pctools.com/security-news/crackers-and-hackers/) on May 15, 2011. Retrieved 2016-09-10.
19. Lloyd, Gene. "Developing Algorithms to Identify Spoofed Internet Traffic". Colorado Technical University, 2014
20. *phreaking* (http://catb.org/~esr/jargon/html/P/phreaking.html). *The Jargon Lexicon*. Retrieved 2008-10-18.
21. *cracker* (http://catb.org/~esr/jargon/html/C/cracker.html). *The Jargon Lexicon*. Retrieved 2008-10-18.
22. Thompson, Ken (August 1984). "Reflections on Trusting Trust" (http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf) (PDF). *Communications of the ACM*. **27** (8): 761. doi:10.1145/358198.358210 (https://doi.org/10.1145%2F358198.358210). S2CID 34854438 (https://api.semanticscholar.org/CorpusID:34854438).
23. Richard Stallman (2002). "The Hacker Community and Ethics: An Interview with Richard M. Stallman" (https://www.gnu.org/philosophy/rms-hack.html). GNU Project. Retrieved 2008-10-18.
24. *Part III. Appendices* (http://catb.org/jargon/html/pt03.html#bibliography). *The Jargon Lexicon*. Retrieved 2008-10-18.
25. *A Story About 'Magic'* (http://catb.org/~esr/jargon/html/magic-story.html). *The Jargon Lexicon*. Retrieved 2008-10-18.
26. *Part III. Appendices* (http://catb.org/jargon/html/pt03.html). *The Jargon Lexicon*. Retrieved 2008-10-18.

Further reading

- Michael Hasse: Die Hacker: Strukturanalyse einer jugendlichen Subkultur (http://elk.informatik.hs-augsburg.de/tmp/cdrom-oss/hasse_hacker.pdf) Archived (https://web.archive.org/web/20170930174851/http://elk.informatik.hs-augsburg.de/tmp/cdrom-oss/hasse_hacker.pdf) 2017-09-30 at the Wayback Machine (1994)

Computer security

- Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.
- Hafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (https://archive.org/details/cyberpunk00kati). New York: Simon & Schuster. ISBN 0-671-68322-5.
- Levy, Steven (2002). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.
- Logik Bomb: Hacker's Encyclopedia (http://insecure.org/stf/hackenc.txt) (1997)

- Revelation: The Ultimate Beginner's Guide to Hacking & Phreaking (http://www.textfiles.com/hacking/ulimate.txt) (1996)
- Slatalla, Michelle; Joshua Quittner (1995). *Masters of Deception: The Gang That Ruled Cyberspace* (https://archive.org/details/mastersofdecepti1994slat). HarperCollins. ISBN 0-06-017030-1.
- Sterling, Bruce (1992). *The Hacker Crackdown* (https://archive.org/details/hackercrackdownl00ster). Bantam. ISBN 0-553-08058-X.
- Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime* (http://insecure.org/stf/them_and_us.txt). Routledge. ISBN 978-0-415-18072-6.
- Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.
- Verton, Dan (2002). *The Hacker Diaries: Confessions of Teenage Hackers* (https://archive.org/details/hackerdiariescon0000vert). McGraw-Hill Osborne Media. ISBN 0-07-222364-2.

Free software/open source

- Graham, Paul (2004). *Hackers and Painters*. Beijing: O'Reilly. ISBN 0-596-00662-4.
- Himanen, Pekka (2001). *The Hacker Ethic and the Spirit of the Information Age* (https://archive.org/details/hackerethic00pekk). Random House. ISBN 0-375-50566-0.
- Lakhani, Karim R.; Wolf, Robert G. (2005). "Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects" (http://ocw.mit.edu/courses/sloan-school-of-management/15-352-managing-innovation-emerging-trends-spring-2005/readings/lakhaniwolf.pdf) (PDF). In Feller, J.; Fitzgerald, B.; Hissam, S.; et al. (eds.). *Perspectives on Free and Open Source Software*. MIT Press.
- Levy, Steven (1984). *Hackers: Heroes of the Computer Revolution*. Doubleday. ISBN 0-385-19195-2.
- Raymond, Eric S.; Steele, Guy L., eds. (1996). *The New Hacker's Dictionary*. The MIT Press. ISBN 0-262-68092-0.
- Raymond, Eric S. (2003). *The Art of Unix Programming*. Prentice Hall International. ISBN 0-13-142901-9.
- Turkle, Sherry (1984). *The Second Self: Computers and the Human Spirit*. MIT Press. ISBN 0-262-70111-1.

External links

- Hacking at Wikibooks
- The dictionary definition of *Hacker* at Wiktionary
- Media related to Hackers at Wikimedia Commons

Retrieved from "https://en.wikipedia.org/w/index.php?title=Hacker&oldid=1023461039"

This page was last edited on 16 May 2021, at 14:41 (UTC).