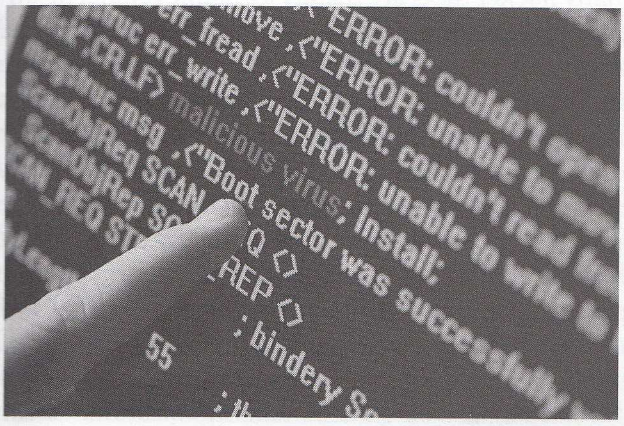
H

Hacking and Hacktivism

Hacking is generally defined as the unauthorized use or entry into a computer or computer system. Hacktivism bridges computer-hacking techniques with political or social protest action. Such actions are sometimes referred to as electronic civil disobedience (ECD). In hacktivism, the hacker is not interested in personal gain but in the dissemination of a particular message. That message may be directed at a particular organization, such as the case in which an anti-fur activist hacked the Website of a furrier, or the Website itself may be inconsequential, serving only as a means of reaching viewers. There are many means by which hacktivism takes place. Common methods include Website defacement, e-mail bombs, and electronic sit-ins or denial-of-service attacks, but these techniques are not universally accepted as ethical within the hacker community.



move ,<"ERROR: couldn't open
err_fread ,<"ERROR: unable to move
err_write ,<"ERROR: couldn't read from
CR,LF> malicious virus; Install:
msg ,<"Boot sector was successfully
ScanObjReq SCAN
ScanObjRep SC
REQ
REP
55 ; bindery Sc

A programmer scans code to determine the location of a system virus. Hackers and hacktivists enter into others' computer systems and perform Website defacement, send e-mail bombs, or cause denial-of-service attacks to demonstrate civil disobedience or to make a statement that information should be free and that authority should not be trusted. (Photos.com)

Website Defacement

In Website defacement, the goal is to break into the system and upload a new version of the page that has been modified by the hackers. However, there is sometimes more to this effort than simply uploading a new web page. If the hackers gain complete access to the system (or "root") they may be able to alter user identification codes and passwords such that the page cannot be taken down until the system administrators are able to break into their own system. This prolongs viewer exposure to the modified page. There are varying degrees of sophistication within the hacker community, and this is reflected in Website defacements. Many defacements are simple messages consisting of the hacker's name and a short note or perhaps a graphic. These are often mass defacements, done by simply scanning networks for servers with open ports or looking for unpatched systems. These hackers seem more interested in disseminating their message as widely as possible, with little consideration of the site itself. On the other hand, some defacements are clearly targeted to send a message to the owner of the Website.

Denial-of-Service Attacks and Electronic Sit-Ins

As the name implies, electronic sit-ins are similar to physical sit-ins: Both seek to deny access by occupying space. Rather than occupying space physically, as in a traditional sit-in, electronic sit-ins occupy space in the form of connections and bandwidth. Servers can handle only as many connections as bandwidth allows. When this connection limit is exceeded, others attempting to access material on that server will be denied access until those who are already connected are no longer accessing material. This is why these kinds of actions are called denial-of-service (DOS) or distributed-denial-of-service (DDOS) attacks. Such attacks are simple to implement and require little skill to enact; some groups, such as Electronic Disturbance Theater, have even automated the process. At its most basic level, a DOS attack can be enacted merely by going to a Web page and continually hitting the refresh button. Most servers can handle this kind of action, but if hundreds or thousands of computers do this, even powerful servers may be brought down.

Because many network attacks are more efficiently mounted using many computers, it is in the interest of the attacker to gain access to many machines—whether through a collective united in the attack or by commandeering the machines of unwitting accomplices. One poorly publicized danger of spyware and viruses has to do with the creation of "zombie networks." Many types of spyware allow for both reception of messages and the transmission of data. If a person has spyware on his or her machine, it is possible to create an exploit that will use the existing spyware to send data to a different server—the target of the attack. This is also a problem of various kinds of viruses, which can install a backdoor into the system that can be used to take over the machine's computing resources, such as bandwidth, processing power, and e-mail send capabilities. A person whose computer is infected with spyware or certain viruses may unknowingly participate in a DOS attack.

E-Mail Bombs

Like DOS attacks, e-mail bombs overload e-mail servers so that legitimate e-mail cannot be received. Most e-mail servers have a set amount of space allocated to each user, and once this limit is reached, no new messages can be delivered. The sender receives an error message and must resend the message later. E-mail bombing is done by sending the recipient many large messages or a very large number of small messages. Some servers limit the size of messages that can be received, thus limiting the tactic to the e-mailing of small messages. Like DOS attacks, e-mail bombs can easily be automated by distributing the resources necessary for the attack.

Hacktivism can take place both on an individual level and through organized "hacktions." One of the most prominent politically active hacker organizations, Cult of the Dead Cow (cDc), claims to have coined the term *hacktivism* through one of its members, Omega. In 1999, cDc began to draw explicit links between activism and computer technology by forming Hacktivismo. Other politically motivated hacking organizations include the Chaos Computer Club (CCC) in Germany; the electrohippie collective, a hacktivist group in the United Kingdom that staged a DOS attack against the World Trade Organization's meetings in 1999; and Electronic Disturbance Theater, whose members used a program called Floodnet to engage in DOS attacks in 1998 on behalf of the Zapatista movement in Mexico.

Although hacktivism seems extremely technical, many hacker tools are readily available online, meaning that one need not actually be a hacker to do the work of the hacktivist. Because hacktivism can be automated, one need not be present to conduct an attack, allowing individuals to protest from another continent if desired. This removes some of the risks inherent in traditional protest actions, which may lead to arrest or injury. However, hacktivism is not without serious risks, not least among which is the potential to incur criminal charges, especially if the act is defined as cyberterrorism. There is also the question of long-term efficacy, especially against a technologically well-defended organization.

Despite its seeming egalitarian nature, there remains the question of access to information technologies to engage in hacktivism. Moreover, the ability to acquire hacking tools does not imply that one has the skills required to use these tools. From a gender perspective, some scholars note that the hacker subculture is largely male-dominated and others have likewise argued that cyberspace itself is largely masculine space.

Brett Lunceford
University of South Alabama

See also Culture Jamming; Cyberpunk; Cyberspace and Cyberculture; Electronic Media and Social Inequality; New Media

Further Readings

Jordan, Tim and Paul A. Taylor. *Hacktivism and Cyberwars: Rebels With a Cause?* New York: Routledge, 2004.

Lane, Jill. "Digital Zapatistas." *TDR: The Drama Review*, v.47/2 (2003).

Ruffin, Oxblood. "Hacktivism, From Here to There." http://www.cultdeadcow.com/cDc_files/cDc-0384.html (Accessed October 2010).

Taylor, Paul A. "Maestros or Misogynists? Gender and the Social Construction of Hacking." In *Dot.Cons*, Yvonne Jewkes, ed. Portland, OR: Willan Publishing, 2003.

Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002.

Wray, Stefan. "On Electronic Civil Disobedience." *Peace Review*, v.11/1 (1999).

Hall, Stuart

Stuart Hall (1932–) is a British cultural theorist, critic, and political strategist whose work centers on intersections between culture, society, and power and the resultant meanings within texts that members of a culture consider as common sense. Hall is one of the most influential theorists responsible for the definition and institutionalization of cultural studies as a separate academic discipline and one of the key figures of the Birmingham Centre for Contemporary Cultural Studies (CCCS) at the University of Birmingham, England, where work in this area was pioneered notably during the 1970s. Hall argues that cultural forms, articulated as texts in mass-media artifacts, convey a preferred or dominant meaning, notably regarding representations of race, culture, ethnicity, and, related to these, gender. Hall sees the technological and social changes of the late 20th century combined with the development of global information and media systems as making even more important the study of their effects on cultural difference and identity.

For Hall, there is no separation between power, culture, and the self. Meanings conveyed by advertisements, film, and television are encoded by their producers as a discourse based on assumptions of what a culture considers important and correct. How these meanings become inculcated into the media products consumed by audiences serves as the foundation for Hall's encoding/decoding model of the communication process, his treatment of cultural hegemony as a process whereby dominant viewpoints become so, and the underlying concept of self versus the "Other" as the basis for stereotyping.

In *Encoding and Decoding in the Television Discourse*, Hall proposes that the mass communication process reflected in television production—and which defines the elements of cultural studies—involves the creation of a message (encoding), which he terms a *sign-vehicle*, and the reception of that message by audience members (decoding). Borrowing from past theorists, Hall notes that the audience serves as both the source and the receiver of a message, because the creators of that message already are members of the same culture as those they are targeting; for shared meaning to occur, the "cultural circuit" must be completed so that the meaning encoded by a message sender is decoded correctly by the receiver. In this sense, the dominant, or "preferred," meaning of a signifying element (either visual or linguistic) is that suggested by the encoder (who works within an institutional structure), although not the one necessarily always decoded by the receiver.

Hall's encoding/decoding model positions meaning—within cultural forms and artifacts—as a product of power and domination, of ideology, popular consciousness, and common sense. The latter two reflect hegemony, which Hall defines as the taken-for-granted knowledge of social structures. Rather than depending on a monolithic, permanent means of control by those in power, hegemony is grounded in a combination of force and consent and remains open to contradictory ideologies (or counterhegemony) and resistance. For Hall, cultural hegemony has to be actively won and secured; it does not result in pure victory or domination, but rather concerns the shifts in the balance of power in relations within