FOR

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

View previous topic :: View next topic

Author	Message
rbc9	Posted: Tue Apr 06, 2004 1:22 pm Post subject: FOR quote edit IP
Joined: 15 Jan 2004 Posts: 2	Diana Massey (dem13) and Rebecca Crotty (rbc9) lab section 2 We contend that the act of gaining unauthorized access to computer systems should not be criminalizedwhen there is no damage. Making this activity illegal will limit “Hacktivism” and Electronic Civil Disobedience. “Hacktivism” is the term coined to describe unauthorized access to computer systems as a way to raise political awareness for social causes. Those who use Electronic Civil Disobedience by definition are nonviolent and not destructive. They find “nonviolent means to expose wrongs, raise awareness, and prohibit the implementation of perceived unethical laws by individuals, organizations, corporations or governments” (Goodrum). Hacktivism strives to stop “the commodification of the internet at the hands of corporate profiteers and violations of human rights at the hands of oppressive governments” (Goodrum). People who intentionally flood websites to raise awareness should not receive the same felony charges as people who using “hacking” as a way to destroy computer systems, or even cause harm or death to the people who own them (Goodrum). Goodrum, Abby and Mark Manion. “Terrorism or Civil Disobedience: Toward a Hacktivist Ethic.” *Computers and Society* (June 2000): 14-19.
Back to top	profile pm email AIM

Display posts from previous: All Posts Oldest First Go

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security All times are GMT - 5 Hours

Page 1 of 1

Watch this topic for replies

Jump to: Debate: Security Go

You **can** post new topics in this forum

Also For

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

View previous topic :: View next topic

Author | Message

nam11

Posted: Tue Apr 06, 2004 2:59 pm Post subject: Also For quote edit

Joined: 13 Jan 2004
Posts: 2
Location: Durham, NC

Names: Desmond Collins, Jasmine Georges, Nikita Mazurov
logins: dtc2, jmg7, nam11
Position: Affirming

Argument:

We hold that gaining unauthorized access to a computer system should not be criminalized (assuming that no damage is done). The exposure of the security hole, will benefit the corporation by pointing out their weaknesses.

Suppose the following scenario:

Someone has gained unauthorized access to a corporation's private database. The intruder has access to the corporation's trade secrets, customer data, and other sensitive information. The intruder, not wanting to do any harm, promptly contacts the corporation and tells them about the security hole they have in their software that allowed him to gain access. The company, knowing of the hole can now try to fix it.

Now, let's assume that the benign intruder does not notify the company, because he is afraid that he will be prosecuted. In about a month, another intruder, albeit not with such a friendly attitude as our first intruder, also finds the same hole and gains access to the same company information. This intruder, takes the information, copies it and sells it to the corporation's competitors.

If the first, benign intruder, had notified the corporation, it would have fixed the security hole and thus no data would have been stolen by the second malignant intruder, who not have been able to access the information.

Thus, by not criminalizing benign attacks, companies in fact save themselves the trouble of having their sensitive data compromised.

References:

Security Focus Homepage. 2004. SecurityFocus. 01 April 2004. http://www.securityfocus.com

Zorz, Mirko. Hackers, Software Companies Feud Over Disclosure of Weaknesses. 15 July 2003. Help Net Security. 01 April 2004. http://www.net-security.org/news.php?id=3121

Back to top

profile pm email www AIM

Display posts from previous: All Posts Oldest First Go

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security All times are GMT - 5 Hours

Page 1 of 1

Watch this topic for replies

Jump to: Debate: Security Go

Don't Legalize It

Author	Message
Steve Poliner (sdp6) Guest	Posted: Tue Apr 06, 2004 3:20 pm Post subject: Don't Legalize It quote edit

Steve Poliner (sdp6)
Jessie Rosario (jdr9)

Against Legalizing

Most critics of criminalizing 'cracking' (gaining unauthorized access to networks or programs) state that the relevant legislation (such as the Digital Millenium Copyright Act of 1998 or the Computer Fraud and Abuse Act of 1984) impedes the creative efforts of scholars and security experts to discover and improve upon flaws in encryption programs and security systems. This is simply not so. Under the DMCA "security testing is limited to those who made a good-faith effort to obtain authorization from the rightholder" (i.e. the ISP or software developer) which is a reasonible and ethical prequisite for attempting to gain access to that network in a pseudo-unauthorized manner. Furthermore, the DMCA though verbose and technical in nature includes "exceptions for encryption research, reverse engineering, and security testing" - provided that efforts have been made to gain authorization from the network provider or service. Moreover, these 'cracking' researchers can still publish what they find to be security flaws on the web or on bulletin boards, but simply cannot disclose completely to the public the process they undertook to access the network - a very reasonable requirement if one is to assume that not every hacker interested in proprietary information is as skillful with a computer as a scholarly expert on security or encryption.

Oft criticized are portions of the DMCA that require corporate stewardship of security for their networks and customer data, in fear that corporations will have little incentive to improve their security if it discovered that there are flaws if these can be kept secret or if upgrades are expensive. Already, though, individual states are providing examples of how such a policy can work - consider, for example, recent legislation requiring companies whose customer data is broken into to notify customers in the state of California, or cases in which Verizon was held liable for failing to upgrade its high-speed internet service to prevent the spread of email

worms. Thus, as is apparent, the criminalization of attempting to access without authorization secure networks is a reasonable policy supported by an evolving body of law that allows experts and those interested in cryptography to continue to assist corporations and the government in maintaining the highest level of data security possible while still preventing those with more base motives from gaining access to secure data.

Quoted passages from Yu, Peter K. "Is Anti-Piracy Law Stifling Cyberspace Innovation?" from Legal Times 3/29/04

Other sources used:
Begun, Eric G. "Worms Spawn Corporate Computer Security Law" New York Law Journal 10/27/03

Altorelli, John J. "New California Law Requires Notification of Security Breaches Involving Personal Information" The Computer & Internet Lawyer 10/03

Text of the DMCA: http://www.copyright.gov/legislation/dmca.pdf

Guide to the CFAA: http://www.informit.com/guides/content.asp?g=security&seqNum=73

Back to top

Display posts from previous: All Posts | Oldest First | Go

newtopic postreply **Duke Computer Science Education Forum Index ->** All times are GMT - 5 Hours
Debate: Security

Page 1 of 1

Watch this topic for replies

Jump to: Debate: Security | Go

You **can** post new topics in this forum
You **can** reply to topics in this forum
You **can** edit your posts in this forum
You **can** delete your posts in this forum
You **can** vote in polls in this forum
You **can** moderate this forum

Go to Administration Panel

Criminalization of Hacking

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

View previous topic :: View next topic

Author	Message
cwa2, dhg2 Guest	Posted: Tue Apr 06, 2004 7:21 pm Post subject: Criminalization of Hacking quote edit

Deedee Grummett (dhg2) & Carrie Alexander (cwa2)
We will debate that the act of gaining unauthorized access to computer systems (cracking) should be criminalized regardless of whether or not damage is incurred.

Arguments:
First of all, cracking violates privacy rights. Nearly all systems contain highly confidential information that, regardless of whether or not it is exploited or damaged, it is not meant to be seen by anyone other than authorized users. In addition, episodes of cracking are extremely damaging financially to companies and corporations involved in e-commerce. Breaches of security are often highly publicized and facilitate the need for extensive PR; often fixing the exposed security issue is neglected or hastily addressed in order to clean up the public relations mess.

References:

Hatcher, Thurston. “Survey: Costs of Computer Security Breaches Soar.” CNN.com. 12 Mar. 2004. Cable News Network LP, LLLP. 30 Mar. 2004 <http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/>.
“Attack ‘may damage public confidence’.” CNN.com. 27 Oct. 2000. Cable News Network LP, LLLP. 29 Mar. 2004. <http://www.cnn.com/2000/WORLD/europe/10/27/microsoft.miles.index.html>.

Back to top

Display posts from previous: All Posts Oldest First Go

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

All times are GMT - 5 Hours

extra arguments

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

View previous topic :: View next topic

Author	Message
dhg2, cwa2 Guest	Posted: Mon Apr 12, 2004 6:58 pm Post subject: extra arguments quote edit

Delegitimatization of Online Communication:
Unlike security technicians authorized by companies to actively seek out and expose security flaws in order to strengthen security, crackers often have malicious intent. If courts fail to criminalize cracking it could render computers an unreliable and unsafe means of communication, when in fact it is one of the most efficient.

Hackers versus Crackers:
According to FOLDOC (http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=hacker), a hacker is "a person who enjoys exploring the details of programmable systems and how to stretch their capabilities," while a cracker is "an individual who attempts to gain unauthorized access to a computer system." While most hackers are simply curious, the line between hacking and cracking can become blurred once a certain level of hacking ability is achieved (i.e. past larval stage). Thus, it is important to prosecute cracking regardless of whether or not damage is incurred in order to discourage hackers from the temptation of cracking.

Back to top

Display posts from previous: All Posts Oldest First Go

newtopic postreply Duke Computer Science Education Forum Index -> Debate: Security

All times are GMT - 5 Hours

Against Legalization of Cracking

Is This A Good Argument?

Yes **100%** [1]
No **0%** [0]

Total Votes : 1

Author	Message
ag58	Posted: Tue Apr 06, 2004 8:42 pm Post subject: Against Legalization of Cracking quote edit
Joined: 21 Jan 2004 Posts: 2	Amod Gautam (ag58) and Robin Singh (rms25) Lab Section 4 Against Legalization of Cracking 1. The explicit threat of the violation of intellectual property rights is very disturbing. For example, there is the great possibility of the theft of trade secrets. Corporations may hire hackers to crack into competing companies and steal their valuable secrets, creating a chaotic free-for-all escalating to cyber warfare. We can take the case of Kevin Mitnik as an example (source: Salkever 00). His case was a controversial and highly publicized criminal-fraud conviction that marked him as the country's most dangerous computer criminal. He's a malicious hacker who broke into computers illegally- can he ever be trusted to help guard sensitive systems for corporate or government clients? "Our company policy is not to hire crackers. We ask all candidates their history with hacking and cracking. We ask them if they have knowingly gained unauthorized access to a system. If they say yes, then we don't hire them," says Stuart McClure, president and chief technology officer of Internet-security consultant Foundstone. Thus, the possibility of the violation of intellectual property rights is very real. 2. Making unauthorized access legal will also open up a proverbial Pandora's Box. Allowing unauthorized access to private computers will only help legitimate hackers. It will make it even easier for those with malicious intent to inflict serious damage because there will be fewer legal consequences. Thus, the negatives may heavily outweigh the positives.

References

1. Salkever, A. (2000, August . Should You Trust a Reformed Hacker? Business Week Online. Retrieved March 31, 2004, from http://www.businessweek.com/bwdaily/dnflash/aug2000/nf2000088_425.htm

2. Elinor Mills Abreu. (2003, September 30). Reuters. Retrieved March 31, 2004, from

http://www.tigertools.net/board/?topic=topic8&msg=1532

3. Hatcher, M., McDannell, J., Ostfeld, S., (1999). Computer Crimes. American Criminal

Law Review. 36 Am. Crim. L. Rev. 397

4. Computer Science and Engineering Department, Florida Atlantic University. (1999,

November 1). Ethics, Appropriate and Illegal Use of CSE Computers at FAU.

Retrieved March 31, 2004, from http://www.cse.fau.edu/resources/ethics.html

5. Ryan Craig and Sergio Chapa. (1996, March 31). Legal and Ethical Issues. Retrieved

March 31, 2004,

from http://home.actlab.utexas.edu/~aviva/compsec/cracker/issues.html

Back to top profile pm email

Display posts from previous: All Posts Oldest First Go

newtopic postreply **Duke Computer Science Education Forum Index ->** All times are GMT - 5 Hours
Debate: Security

Page 1 of 1

Watch this topic for replies

Jump to: Debate: Security Go