Santa Clara High Technology Law Journal

Volume 16 | Issue 2 Article 1

January 2000

Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws

Eric J. Sinrod

William P. Reilly

Recommended Citation

Eric J. Sinrod and William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara High Tech. L.J. 177 (2000).
Available at: http://digitalcommons.law.scu.edu/chtlj/vol16/iss2/1

ARTICLES

CYBER-CRIMES: A PRACTICAL APPROACH TO THE APPLICATION OF FEDERAL COMPUTER CRIME LAWS

Eric J. Sinrod[†] **and William P. Reilly**[††]

TABLE OF CONTENTS

[†] Eric J. Sinrod is a partner focusing on e-commerce issues in the San Francisco office of the national law firm Duane, Morris & Heckscher LLP. Mr. Sinrod can be reached at EJSinrod@duanemorris.com.

[††] William P. Reilly is a law student at the University of San Francisco and has a background in e-commerce and computer security. Mr. Reilly can be reached at WPReilly@duanemorris.com.

I. INTRODUCTION

Cyber-crime, once the domain of disaffected genius teenagers as portrayed in the movies "War Games" and "Hackers," has grown into a mature and sophisticated threat to the open nature of the Internet. "Cyber-criminals," like their non-virtual traditional criminal counterparts, seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with reports of debilitating denial of service attacks, defaced web sites, and new computer viruses worming their way through the nation's computers. However, there are countless other cyber-crimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security.[1]

Along with the phenomenal growth of the Internet has come the growth of cyber-crime opportunities.[2] As a result of rapid adoption of

[1] Michael Hatcher et al., *Computer Crimes*, 36 AM. CRIM. L. REV. 397, 399 (1999).

[2] *See* Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839 (1999). In a recent survey of 643 computer security practitioners in the U.S., "[s]eventy percent reported a variety of serious computer security breaches other than the most common ones of computer viruses, laptop theft or employee 'net abuse' -- for example, theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks and sabotage of data or networks." Computer Security Insititute, *Ninety percent of survey respondents detect cyber attacks, 273 organizations report $265,589,940 in financial losses* (Mar. 22, 2000) <http://www.gocsi.com/prelea_000321.htm> [hereinafter CSI Survey]. The report also found that:

> Ninety percent of respondents (primarily large corporations and government

the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.[3] Law enforcement officials have been frustrated by the inability of legislators to keep cyber-crime legislation ahead of the fast-moving technological curve.[4] At the same time, legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.[5]

Further complicating cyber-crime enforcement is the area of legal jurisdiction.[6] Like pollution control legislation, one country can not by itself effectively enact laws that comprehensively address the problem of Internet crimes without cooperation from other nations. While the major international organizations, like the Organisation for Economic Co-operation and Development (OECD) and the G-8, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cyber-crime for many reasons, including different values concerning piracy and espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber-criminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another.

In section II of this article, we begin by providing an overview of cyber-crimes, the state of the law, and cyber-crime perpetrators and their motivations. Then, in section III we discuss in detail three major computer crimes and analyze how the different statutory subsections are applied depending upon the technical details of the crime itself. Just as a murder prosecution is dependent on *how* the crime was committed, different hacking techniques trigger different federal anti-

> agencies) detected computer security breaches within the last twelve months . . . [s]eventy-four percent acknowledged financial losses due to computer breaches . . . [and] [f]orty-two percent were willing and/or able to quantify their financial losses. The losses from these 273 respondents totaled $265,589,940 (the average annual total over the last three years was $120,240,180).

Id.

[3] *See Federal Law Enforcement Response to Internet Hacking: Hearing of the Commerce, Justice, State and Judiciary Subcomm. of the Senate Appropriations Comm.*, 106th Cong. (2000) [hereinafter *Federal Response to Hacking*] (statement of Louis Freeh, Director, Federal Bureau of Investigation).

[4] *See id.*

[5] There is concern that the effort to fill the legal vacuum will include some protected rights, as was demonstrated by the Supreme Court's holding in *Reno v. ACLU*, 521 U.S. 844 (1997).

[6] *See* Lee et al., *supra* note 2, at 873.

computer crime subsections. We begin with a discussion of the various denial of service attacks and the applicable statutes. Next we discuss the technical details of several hacking techniques and apply the relevant statutory subsections to the specific techniques. Finally, we explore the various types of computer viruses and how viral "payloads" and the class of the targeted computer will determine which federal subsection can be applied to the crime. In section IV, we discuss proposed legislative changes to the Computer Fraud and Abuse Act and related privacy concerns. Finally, we conclude this paper with a brief statement on the importance of tying together the technical elements of a cyber-crime and the application of the appropriate criminal subsection.

II. BACKGROUND

What is a cyber-crime? Law enforcement experts and legal commentators are divided. Some experts believe that computer crime is nothing more than ordinary crime committed by high-tech computers and that current criminal laws on the books should be applied to the various laws broken, such as trespass, larceny, and conspiracy. Others view cyber-crime as a new category of crime requiring a comprehensive new legal framework to address the unique nature of the emerging technologies and the unique set of challenges that traditional crimes do not deal with; such as jurisdiction, international cooperation,[7] intent, and the difficulty of identifying the perpetrator. Another source of confusion is the meaning of "hacker" and "cracker" and the distinction behind their motivations. The following section will elaborate on the differences between the two and their relevance to federal criminal statutes.

A. *The State of the Law*

Congress has approached computer crime both as traditional crime committed by new methods and as crime unique in character requiring new legal framework. For example, Congress has amended the Securities Act of 1933[8] to include crimes committed by a computer. However, Congress has also enacted a comprehensive new computer fraud and abuse section that can easily be amended to reflect changes in technology and computer use by criminals. In fact, the U.S. Congress has enacted statutes that widen the scope of

[7] Michael A. Sussmann, *The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 453-55 (1999).

[8] 15 U.S.C. § 77(a)-(aa) (1994).

traditional crimes to specifically include crimes involving computers, or categorize them as entirely separate offenses. For example, the main federal statutory framework for many computer crimes is the Computer Fraud and Abuse Act (CFAA).[9] The statute is structured with an eye to the future so that it can be easily amended to reflect changes in technology and criminal techniques. The statute has already been amended several times to close unintended loopholes created by judicial interpretation. In its current form, the statute is very broad in scope, reflecting the government's resolve to combat cyber-crime at every level.

B. The Perpetrators—Hackers and Crackers

1. Hackers

"Hacker"[10] is a term commonly applied to a "computer user who intends to gain unauthorized access to a computer system."[11] Hackers are skilled computer users who penetrate computer systems to gain knowledge about computer systems and how they work.[12] The traditional hacker does not have authorized access to the system.[13] Hacking purists do not condone damage to the systems that are hacked.[14] According to The Jargon Dictionary, the term "hacker" seems to have been first adopted as a badge in the 1960s by the

[9] 18 U.S.C.A. § 1030 (West Supp. 1999).

[10] The term "hacker" has been defined as "[a] computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance." WEBSTER'S NEW WORD DICTIONARY OF COMPUTER TERMS 235 (7th ed. 1999). See Appendix A for a more detailed definition.

[11] Michael P. Dierks, *Symposium: Electronic Communications and Legal Change, Computer Network Abuse*, 6 HARV. J. L. & TECH. 307, 310 n.7 (1993).

[12] According to Deb Price and Steve Schmadeke, the "Hackers credo" is:

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

Deb Price & Steve Schmadeke, *Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive*, DET. NEWS, Feb. 14, 2000, at A1, *available in* 2000 WL 3467302.

[13] However, this is not a legal distinction. The Computer Fraud and Abuse Act criminalizes unauthorized access and access that exceeds authorization. *See* 18 U.S.C.A. § 1030(a)(1) (West Supp. 1999).

[14] *See* Dissident, *Ethics of Hacking* (visited Mar. 3, 2000) <http://cultdeadbunnies.virtualave.net/hacking/lit/files/ethics.txt>.

hacker culture surrounding The Tech Model Railroad Club (TMRC) at Massachusetts Institute of Technology when members of the group began to work with computers.[15] The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.[16]

In the hacking "community," it is considered better to be described as a "hacker" by others than to describe oneself as a "hacker."[17] Hackers consider themselves members of an elite meritocracy based on ability and trade hacker techniques and "war stories" amongst themselves in Usenet forums, local or regional clubs, and national conferences, such as the annual Def Con Computer Underground Convention held in Las Vegas.[18]

2. Crackers

A "cracker" is a hacker with criminal intent.[19] According to The Jargon Dictionary,[20] the term began to appear in 1985 as a way to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers[21] maliciously sabotage computers, steal information located on secure computers, and cause disruption to the networks for personal or political motives.[22]

Estimates made in the mid-1990's by Bruce Sterling, author of *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, put "the total number of hackers at about 100,000, of which

[15] *See* The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/h.html#hacker>.

[16] *See generally* STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 10 (1984).

[17] *See* Appendix A.

[18] DEF CON is an annual computer underground party and conference for hackers held every summer in Las Vegas, Nevada. *See* DEF CON (visited Apr. 5, 2000) <http://www.defcon.org>.

[19] The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/c/cracker.html>.

[20] *See* Appendix A.

[21] Please note that a "cracker" is different from a "crack." A crack is a script that defeats software protection codes, as opposed to using a circulated password that allows installation of the software. As software protection techniques become more sophisticated, the use of "cracks" have gained in popularity, as well as the challenge amongst crackers to defeat the protections. Most popular software passwords and/or cracks are widely available on the Internet. For example, one can quickly find software cracks by running a search on Astalavista (visited Mar. 9, 2000) <http://astalavista3.box.sk/>.

[22] This distinction does not mean that hackers do not cause damage, but often it is their lack of intent that sets them apart from crackers, even though federal law does not always make such a distinction. *See* discussion *infra* on 18 U.S.C.A. § 1030 (West Supp. 1999).

10,000 are dedicated and obsessed computer enthusiasts. A group of 250-1,000 are in the so-called hacker 'elite', skilled enough to penetrate corporate systems and to unnerve corporate security."[23]

In the eyes of the law, hacking and cracking are not always treated the same way. Depending upon the method of intrusion, the type of computer that was broken into, the hacker's intent, and the type and amount of damage, different statutes and penalties will apply.[24] There are many ways to approach a discussion on hacking. In this article, we will structure the discussion on hacking techniques within the framework of the statutory elements to provide an understanding of how the different techniques trigger different statutes and penalties. We begin with an overview of hacking and an explanation of several common hacking techniques. Then, we discuss the relevant criminal code that can be applied depending on the nature of the hack.

C. Why People Hack

1. Hactivism

In recent years, according to the Department of Justice's National Infrastructure Protection Center, there has been a rise in what has been dubbed "hacktivism." Hacktivists launch politically motivated attacks on public web pages or e-mail servers. The hacking groups and individuals, or Hacktivists, overload e-mail servers by sending massive amounts of e-mail to one address and hack into web sites to send a political message.[25] In 1999, for example, the homepages for the White House, the U.S. Department of the Interior, White Pride, the United States Senate, Greenpeace, and the Ku Klux Klan were attacked by political activists protesting the sites' politics.[26]

[23] *Cyberterrorism Hype*, JANE'S INTELLIGENCE REV., Dec. 1, 1999, at 48, 49, *available in* 1999 WL 8946130.

> However, to launch a sophisticated attack against a hardened target requires three to four years of practice in C, C++, Perl and Java (computer languages), general UNIX and NT systems administration (types of computer platform), LAN/WAN theory, remote access and common security protocols (network skills) and a lot of free time. On top of these technical nuts and bolts, there are certain skills that must be acquired within the cracker community.

Id.

[24] *See* 18 U.S.C.A. § 1030(c) (West Supp. 1999).

[25] *See Senate Joint Cyberattack Investigation: Capitol Hill Hearing Testimony*, 106th Cong. (2000) [hereinafter *Cyberattack Investigation*] (statement of Michael Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

[26] *See Flashback Sweden* (visited Mar. 12, 2000) <http://www.flashback.se/hack/1999/>.

One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line to raise awareness for its political agenda regarding the Zapatista movement in Mexico and other issues.[27] Also, during the 1999 NATO conflict in Yugoslavia, hackers attacked web sites in NATO countries, including the United States, using virus-infected e-mail and other hacking techniques.[28] On February 7, 2000, the official web site of the Austrian Freedom Party was hacked to protest the inclusion of Jörg Haider and his party into a coalition Austrian government.[29]

2. Employees

According to a study conducted in 1999 by Michael G. Kessler & Associates Ltd., disgruntled employees are the greatest threat to a computer's security.[30] Employees that steal confidential information and trade secrets account for thirty-five percent of the theft of proprietary information.[31] In fact, data suggests that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to outside hackers with modems.[32] Internet Security Systems' Chris Klaus estimates that over eighty percent of the attacks on computer systems are committed by employees.[33]

According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes.[34] Insiders do not need a great deal of knowledge about their target computers, because their inside knowledge of the victim's system allows them unrestricted access to

[27] *See Federal Response to Hacking, supra* note 3.

[28] *See id.*

[29] To view a copy of the hacked web site, see (visited Apr. 9, 2000) <http://www.flashback.se/hack/2000/02/07/1/>.

[30] *See* David Noack, *Employees, Not Hackers, Greatest Computer Threat* (Jan. 4, 2000) <http://www.apbnews.com/newscenter/internetcrime/2000/01/04/comptheft0104_01.html>.

[31] *See id.*

[32] *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalizaton: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116 (1988).

[33] Matthew Nelson, *Internet Security Systems' Chris Klaus says companies should close back doors to be secure*, INFOWORLD, Jan. 10, 2000, at 40a. According to a recent survey of 643 computer security practitioners in the U.S., 71% reported unauthorized access by insiders. *See* CSI Survey, *supra* note 2.

[34] *See* Congressional Statement, Federal Bureau of Investigation, *National Infrastructure Protection Center (NIPC) Cyber Threat Assessment, October 1999, Before the Subcomm. on Technology and Terrorism of the Senate Comm. on the Judiciary* (Oct. 6, 1999) <http://www.y2kcoming.com/cyber/nipc10_99.htm> (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

cause damage to the system or to steal system data.[35] A Computer Security Institute/FBI report notes that fifty-five percent of survey respondents reported malicious activity by insiders.[36] Employees who exceed their authorized use and intentionally cause damage are just as liable as an outside hacker who intentionally causes damage.[37] However, § 1030(a)(5) of the CFAA does not criminalize damage caused by authorized persons and company insiders that was reckless or negligent.[38] Only outside non-authorized hackers are liable for *any* damage caused, whether it was negligent, reckless, or intentional.[39]

3. Recreational Hackers

"Recreational hackers" break into computer networks for the thrill of the challenge or for bragging rights in the hacking community.[40] While hacking once required a fair amount of skill or computer knowledge, the recreational hacker today can now download attack scripts and protocols from the Internet and launch them against victim sites with little knowledge of the systems they are attacking.[41] There are countless web sites on the Internet that provide "newbies" (inexperienced hackers, or "wannabes") with detailed instructions on hacking techniques and downloadable, do-it-yourself hacking tools.[42] In recent years, the hacker's attack tools have become more sophisticated and easier to use.[43] For example, in 1999 hackers defaced the Anniston Army Depot, Lloyd's of London, the U.S. Senate and Yahoo home pages to demonstrate to the hacking community their ability to hack into third-party servers and to highlight the servers' vulnerabilities.[44]

[35] *See id.*

[36] *See id.*

[37] 18 U.S.C.A. § 1030 (West Supp. 1999).

[38] *Id.* § 1030(a)(5).

[39] *See id.* § 1030(a)(5)(C).

[40] *See Cyberattack Investigation, supra* note 25.

[41] *See* Internet Security Systems, *Back Orifice 2000 Backdoor Program* (visited Apr. 5, 2000) <http://www.iss.net/customer_care/resource_center/whitepapers> [hereinafter *Back Orifice*].

[42] Hackers learn hacking techniques from a variety of sources, including high school and university computer groups; newsgroups such as alt.2600.hackerz and alt.binaries.hacking.beginners; hacking web sites such as <http://www.flashback.se> and <http://www.lopht.com/>; as well as hacking search engines, such as <http://astalavista.box.sk/>.

[43] *See Cyber Threat Assessment, supra* note 34.

[44] *See Flashback Sweden, supra* note 26.

4. Web Site Administrators and Web Pages

It is usually considered a passive and harmless exercise to visit a web site. The user requests information and the server responds to the request by sending out packets of requested data back to the user's computer. However, web sites can also access a lot of hidden background information from the user. For example, Privacy.net has a web site that will show users all of the information that can be taken from their individual computer.[45] The remote web site can determine the following information about a visitor:

(a) the IP address the user is accessing the web site from;

(b) the number of prior visits to the web site, and the dates;

(c) the URL of the page that contained the link to get the user to the web site;

(d) the user's browser type and operating system and version;

(e) the user's screen resolution;

(f) whether JavaScript and VBScript are enabled on the user's computer;

(g) how many web pages the user has visited in the current session;

(h) the local time and date; and

(i) FTP username and password, if there is one.[46]

Privacy advocates have pressured web browser developers to address security concerns by enabling users to significantly enhance their privacy by adjusting the security level on their browsers. The extent of information that a web site can retrieve from a visitor without violating the CFAA is still uncertain. Section 1030(a)(2)(C) proscribes the intentional access of computer information. When a person visits a web site, how much information has that person reasonably "authorized" the web site to obtain? This question may be answered by a court in one of the cases filed against RealNetworks over its gathering of user data.[47]

[45] *Privacy.net: The Consumer Information Organization* (visited Mar. 5, 2000) <http://privacy.net/analyze/>.

[46] *Id.*

[47] In November, 1999, it was alleged that "RealNetworks' popular RealJukebox software ... surreptitiously monitors the listening habits and certain other activities of people who use it and continually reports this information, along with the user's identity, to RealNetworks." Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, N.Y.

It is also possible for a web programmer to enable a web page to send an e-mail to a predetermined address just by visiting the page through a JavaScript exploit in Netscape Navigator Versions 2.0 through 4.0b1.[48] For example, if a person visits such a web site, hidden within the hypertext markup language (HTML) is code that will cause the person's e-mail program to send an e-mail to the web site with the person's e-mail address in the "from" slot. Theoretically, this exploit would allow a web site to collect all of the e-mails from persons who visit their web site. Internet Explorer and Netscape Navigator provide security warnings to users before they send the mail if the security level is set at a higher level.[49]

III. TYPES OF COMPUTER CRIME

In this section, we begin by providing an overview of cyber-crime and criminal techniques used to penetrate protected computer networks, including: (1) Denial of Service attacks; (2) web site defacing and malicious interference; and (3) malicious code—viruses, worms, and Trojans. We then discuss in detail the CFAA, how it is applied, and how it has changed over the past decade. We also look at other laws that the federal government uses to control computer crimes.

A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense.[50] An understanding of the different uses of a computer will provide the foundation of the application of the criminal statutes.

The computer is an indispensable tool for almost all cyber-

TIMES, Nov. 1, 1999 at C1. A security expert discovered that RealNetworks was using its RealJukebox player to secretly scan the hard drives of computers and send the information about the user's musical content and preferences to the company. The software also created a serial number to identify the user. *See id.* As a result, three class-action lawsuits were filed against RealNetworks. Two federal lawsuits, filed in Pennsylvania and Illinois, alleged that the company violated the Computer Fraud and Abuse Act by secretly collecting personal information without the user's consent. The lawsuits claim that this is a violation of federal law because RealNetworks accesses information on a protected computer without the knowledge of the user. *See* Greg Miller, *RealNetworks Breached Privacy, 3 Suits Contend Consumers: Firm Admitted Collecting Data on Users of its Internet Software, Provoking the First Class Actions in Such a Case*, L.A. TIMES, Nov. 11, 1999, at C1.

[48] *See DigiCrime E-mail Address Demonstration* (visited Mar. 5, 2000) <http://www.digicrime.com/noprivacy.html>; *see also Onion Routing* (visited Mar. 5, 2000) <http://www.onion-router.net/Tests.html> (listing other good privacy testing sites).

[49] For example, Microsoft Internet Explorer provides four levels of security on its web browser, ranging from low to high. The various levels of security allow the user to make a tradeoff between unimpeded access to all Internet content and security concerns.

[50] *See* Hatcher et al., *supra* note 1, at 401.

crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply.[51]

When a computer is the target of the offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system, or computer network.[52] Hacking, cracking, espionage, cyber-warfare, and malicious computer code viruses are common forms of crimes that target the computer. The perpetrators range from teenage "cyber-joyriders" to organized crime operations and international terrorists. According to a survey conducted by Michael G. Kessler & Associates Ltd., a New York security firm, computer theft of proprietary information is committed by discontented employees (35%), outside hackers (28%), other U.S. companies (18%), foreign corporations (11%), foreign governments (8%), and miscellaneous (10%).[53]

The computer may also be a tool of the offense. The criminal uses the computer to commit a traditional crime, such as counterfeiting. For example, a counterfeiter that used to engrave plates to create the counterfeit currency can now use sophisticated graphic computers with advanced color printers. An example of a computer used to perpetrate a traditional crime is the extortion attempt by George Matos Rocha from North Carolina.[54] Mr. Rocha was charged with bombing three home improvement stores and subsequently threatened the retail chain to continue the bombings unless he received $250,000.[55] Using the Internet, Mr. Rocha set up a bank account in Latvia and instructed the company to wire the extortion money to his Latvian account.[56] The FBI was able to identify the account and trace its origin back to the United States with the help of his Internet Service Provider. Mr. Rocha pleaded guilty in

[51] L0pht Heavy Industries is developing a hacking platform based on the PalmPilot, mainly because of its high-mobility and the ability to communicate with desktop computers. L0pht already offers several applications for PalmPilots that demonstrate its potential as the next hacker's development platform. The ability to communicate using wireless infrared communication, the small size and the support for TCP/IP makes PalmPilot almost ideal for physical penetration to a local network. *See LØPHT Heavy Industries* (visited Mar. 19, 2000) <http://www.lopht.com>; *see also* Phil Askey, *How to Connect Your PalmPilot to Windows NT*, Jagtech (1997) <http://www.jagtech.com.au/Docs/pilot_nt.htm> (copy on file with the author).

[52] *See id.*

[53] *See* Noack, *supra* note 30.

[54] *See* Paula Christian, *Lowe's Bombing Suspect Pleads Guilty; A Greensboro Man Will Face at Least 37 Years in Prison When He is Sentenced in March*, GREENSBORO NEWS AND REC., Dec. 7, 1999, at A1, *available in* 1999 WL 26311607.

[55] *See id.*

[56] *See id.*

December to explosives charges and extortion. He could have faced life in prison.[57]

Computers can also be incidental to the offense, but are nevertheless important because they contain the evidence of a crime. Money launderers, for example, may use a computer to store details of their laundering operation instead of relying on paper accounting records. Child pornographers' computers are often seized as the key evidence[58] that the defendant produced, possessed, received, and/or distributed child pornography.[59]

A. *Denial of Service*

A Denial of Service (DoS) attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to "bring down" a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to these attacks, a basic understanding of the anatomy of the attacks is

[57] *See 40 Years Meted in Lowe Bombings*, *in* Henry Bailey, U.S. & WORLD NEWS IN BRIEF, COM. APPEAL (Memphis TN), Mar. 10, 2000, at A5, *available in* 2000 WL 4444494.

[58] *See, e.g.*, United States v. Snyder, 189 F.3d 640 (7th Cir. 1999). James Snyder was convicted of producing, receiving, and distributing child pornography, as well as possessing child pornography with intent to sell. Mr. Snyder engaged in a sexual affair with a minor child. After the minor was interviewed by the FBI and was able to describe the abuse and identify Mr. Snyder's house, a search warrant was obtained and served on Mr. Snyder. The computer-related evidence seized from Snyder's house was "analyzed by the FBI crime lab . . . [and] verified that Snyder's computer was capable of downloading and uploading images from the Internet, and that it could be hooked up to a camera. [The FBI] also recovered several pornographic images from the computer, even though they had been deleted." *Id.* at 644.

[59] *See, e.g.*, United States v. Simons, 29 F. Supp. 2d 324 (E.D. Va. 1998). Mark Simons was an employee of the Foreign Bureau of Information Services (FBIS) component of the CIA. While a FBIS network administrator was doing a routine check of the agency's firewall, he noticed a lot of activity from one work station going to a pornographic site, against established agency rules. The computer was seized as evidence and Mr. Simons was charged with violating 18 U.S.C. § 2252A(a)(2)(A) (1994), Receiving Materials Containing Child Pornography, and 18 U.S.C. § 2252A(a)(5)(B), Possession of Material Containing Child Pornography. Mr. Simons unsuccessfully challenged the seizure on grounds that the search was a violation of the Fourth Amendment. The court held that, in applying the holding in *Katz v. United States*, 389 U.S. 347 (1967), the court must consider "whether the employee searched had a reasonable expectation of privacy. The person must have had an actual or subjective expectation of privacy and the expectation must have been one that society recognizes as reasonable." United States v. Simons, 29 F. Supp. 2d at 326-27. The FBIS has a specific policy providing for computer audits and given this policy, the court concluded that Mr. Simons did not have a "reasonable expectation of privacy with regard to any Internet use." *Id.* at 327.

necessary.[60]

There are basically three main network exploits that are used to overwhelm a system's server: SYN Flood Attacks, UDP Flood Attacks and ICMP Flood Attacks. Each technique exploits a weakness in the way computers communicate amongst each other over the Internet. A basic understanding of the TCP/IP Internet protocols is helpful to differentiate between the techniques.

Internet Protocols:

The Internet is a network of computers that are connected so they can exchange information amongst each other. The computer that is asking for information from another computer is the "client" and the computer that is receiving the request is the "server." When the client wants to receive information that is located on the server, it sends a request for the information. However, the computers must establish a connection before data can be exchanged. The server needs to know who it is going to send the information to and needs to make sure the client computer is ready to receive the information. This is considered a "3-way handshake." The first part of the handshake occurs when the client computer sends a message to the server with a "SYN flag" that tells the server how to identify it.[61] Second, upon receiving the request, the server will send out its own identification number, called an Initial Sequence Number (ISN) in a SYN for this request and an acknowledgement (ACK) of the client's request. In the third part of this "handshake," the client computer receives the SYN and ACK from the server and sends back the ACK with the server's numbers, like a secret code the two of them share so the server can keep track of multiple clients. Now the data transfer can take place. In summary, the client sends a message to the server, the server sends back a message to the client that the server is "awake" and ready to process the requests, then the client sends back an acknowledgement that it is ready to receive. This may seem redundant, but the need to establish the connection on both sides is

[60] Many commentators equate a DoS to a store front being blocked by hundreds of protestors to deny legitimate customers from entering the store. A more accurate analogy would be sending a hundred people into a store who overwhelm the sales staff, rendering them unable to respond to legitimate customers. Eventually, the store becomes so crowded that a line forms outside, where the "bogus" customers and real customers queue up, denying access to legitimate customers.

[61] A "SYN" packet is an abbreviation for "synchronized/start." The SYN packet is the packet that originates with the "source host," or the person initiating the communication. The SYN packet is part of the TCP "3-way handshake."

very important, because the data is broken up into small packets by the server and sent out over the Internet to the client. The client needs to know how to organize the data puzzle as the packets arrive and the client also needs to know if any packets are missing. As each piece of the puzzle arrives, the client lets the server know the piece has been received, so the server knows if it has to re-send it.

TCP/IP stands for Transmission Control Protocol and Internet Protocol.[62] Basically, the TCP is the workhorse of the communication on both sides. If a file is requested by the client, the server locates the file on its computer and breaks the file into tiny pieces. The tiny pieces are called datagrams. Each datagram is "wrapped" in a bundle of instructions that tells it where to go. These little bundles are called "packets." The TCP assigns a sequence number to every byte transferred so it can track what it has sent and eliminate the need to duplicate sending the same packet twice unless the packet is lost somewhere along the line to the client. The "packet header," contains the sequence numbers that also tells the client the next sequence number to expect after each packet, so the client can start arranging the packets and conduct a rolling inventory. The TCP acts as a digital shipping and receiving department.

The job of the Internet Protocol (IP) is easier. The IP's job is to route the packets across the Internet to the client. Each computer on the Internet has an IP address that tells the computers where the other is located. The IP address is very similar to a zip code. For example, a zip code that begins with a 9, belongs to an address located on the west coast of the United States. If the next number is a 4, the location is in the San Francisco area, and so on until the precise region is located. However, to parallel the IP addresses, each house in the zip code area would be assigned a number, instead of an address. So when a client or server sends a packet out over the Internet, the packet is "routed" through many other servers to reach its final destination. The IP tacks on the numerical address and ships it out, hoping the packet arrives where it is supposed to go. If the server does not receive a response that the packet was received on the other end, the IP can send an error message to the client, called an Internet Control Message Protocol, or ICMP, letting the client know that the packet did not get there. It is this system of trust and cooperation between the computers that is exploited by a denial of service attack.

[62] *See* Appendix A.

1. SYN Flood Attacks

One of the weaknesses in the system is the amount of SYN requests the TCP can handle. When the TCP receives more requests than it is programmed to handle, it puts the other incoming SYN requests in a queue. When the queue is filled to capacity, there is no more room to put the other incoming SYN requests and they are turned back. Hence, they are "denied service."

Another technique is to slow down the TCP process by making the TCP wait for all of the ACKs it sent out to be acknowledged by the client. When the attacker sends a message to the server requesting data, the server sends out a SYN and an ACK and waits to hear back from the attacker's client, as part of the third part of the 3-way handshaking. However, the attacker has "spoofed" his return address so that the server sends a "self-addressed and stamped" envelope to an address that is either false or belongs to a computer that is not responding. If enough of these "spoofed" SYN messages are sent, the server is paralyzed by its wait for non-existent confirmations. "SYNK" is a common SYN flood program that is widely downloadable on the Internet.[63]

2. UDP Flood Attacks

User Datagram Protocol (UDP) flood attacks work in very much the same manner as the SYN Flood attacks. In a server, the UDP provides information about the server to other computers, such as the server's local time, echo, chargen, etc.[64] When the server is hit with multiple requests for information about itself, the server can be quickly overwhelmed by its inability to process so many UDP packets. The result is total consumption of the server's processing power and bandwidth, thereby "denying service" to others who are trying to access the server. The problem is multiplied when a hacker connects one computer's chargen port with another's echo port. The result is the generation of a massive amount of packets that overwhelm the system and render it useless.[65]

[63] SYNK, along with other DoS tools, is available on many hacking web sites. For example, SYNK can be obtained at Warmaster's web site. *See Warmaster* (visited Apr. 5, 2000) <http://www.warmaster.de/linw.htm>.

[64] For example, the UDP "echo" provides a port that returns every packet sent to it. The UDP "chargen" returns a packet with 0 to 512 characters chosen randomly. The UDP "time" protocol provides the time in a site-independent, machine readable format. The client sends an empty datagram to the port, and the server sends a datagram containing the time as a 32 bit binary number.

[65] *See CERT Coordination Center Report CA-96.01: UDP Port Denial-of-Service Attack*

3. ICMP Flood Attack

The Internet Control Message Protocol (ICMP) flood attack is also similar to the above flood attacks. The ICMP is used to handle errors and "pings." Pings are small "feelers" that are sent out to other computers to see if they are turned on and connected to the same network.[66] Ping is also used to determine if there is network congestion and other network transport problems. When a ping packet is sent to an IP broadcast address from a computer outside of the remote computer's network, it is broadcast to all machines on the target network.

The ICMP attack begins when a large number of forged ping requests are sent to a broadcast address on a third-party's server. These packets contain the return address of the intended victim. The flood of ping requests causes the targeted server to answer with a flood of responses which can cause both the target site and third-party sites to crash.[67]

A variation on the ICMP attack is the "Ping of Death." The Ping of Death is a large ICMP packet that is sent to the target server. The target receives the ping in fragments and starts to re-assemble the packets as they arrive. However, the completed size of the packet is larger than the buffer, or than the room the computer has allocated to such packets, and the computer is overwhelmed, often resulting in the server shutting down or freezing up.[68]

4. New Generation Attacks

a. Smurf Attacks

These techniques are named after the programs that launch the

(visited Mar. 17, 2000) <http://www.securityfocus.com/templates/archive.pike?list=21&date=1996-02-08&msg=v02120d01ad4092622ff2@[128.115.138.237]>.

[66] *See GUIDE TO (mostly) HARMLESS HACKING* (visited Mar. 12, 2000) <http://newdata.box.sk/neworder/harmless/GTMHH2-3.TXT>.

[67] As an example of this type of attack, consider the following: To launch a ping attack, the attacker, using Computer A, gets the IP address of a computer he wants to bring down. If Computer A is using Windows, all the attacker needs to do is go to the DOS prompt and enter "c:\windows\ping -1 65510 targeted.computer.com." This command creates a giant datagram that gets wrapped inside a packet that is sent to targeted.computer.com and overloads the targeted computer as it tries to send the pin back. It is a very simple technique, and just as easy to get caught if the attacker used his computer to launch the ping attack. However, the attacker will typically spoof his location, making discovery more difficult.

[68] *See The Hack FAQ - Denial of Service Basics* (visited Mar. 12, 2000) <http://www.nmrc.org/faqs/hackfaq>.

attacks. In a Smurf attack, the hacker sends out an ICMP echo request packet, or "ping" command to a computer network with the return IP address of the targeted victim. The network's server broadcasts the "ping" through the system's network and the computers send a reply back. If the network is large enough, those packets will swamp the victim's computer and possibly bring the computer down.[69]

b. Fraggle

The Fraggle attacks are similar to the Smurf attacks, except they use UDP echo packets to overwhelm a network computer.

c. Papasmurf

Papasmurf combines Smurf and Fraggle by launching ping requests with ICMP echo packets and UDP echo packets. This program's two-headed assault makes it more difficult for administrators to defend themselves.

5. Distributed Denial of Service Attacks

Distributed Denial of Service attacks (DDoS) are a natural development in the search for more effective and debilitating denial of service attacks. Instead of using just one computer to launch an attack, the hacker enlists numerous computers to attack the target computer from numerous launch points.[70] Prior to an attack, the hacker places a daemon, or a small computer program, on an innocent third-party computer. These third-party computers are often referred to as "zombies" or "soldiers." The "slave" daemons are remotely controlled by the "master" program to launch attacks against certain servers. By distributing the source of attacks across a wider array of zombie computers, the attacker has made it more difficult for the target server to block off the attack routes.

a. Trinoo (June 1999)

On August 17, 1999, a Trinoo network of at least 227 systems was used to flood a single server at the University of Minnesota, including more than 100 compromised computers at the University of

[69] *See* Carnegie Mellon Software Engineering Inst., *CERT® Advisory CA-98.01 "smurf" IP Denial-of-Service Attacks*, (originally issued Jan. 5, 1998) (last modified Mar. 13, 2000) <http://www.cert.org/advisories/CA-98.01.smurf.html>.

[70] *See* Brian Martin, *Have Script, Will Destroy (Lessons in Dos)*, HACKER NEWS (visited Mar. 13, 2000) <http://www.hackernews.com.bufferoverflow/00/dosattack/dosattack.html>.

Washington.[71] The attack rendered the system inoperable for two days.

There has been speculation that Trinoo was one of the programs that brought down Yahoo and other major Internet sites in February 2000.[72] Trinoo is used to create distributed denial of service UDP flood attacks. There is concern that Trinoo could enlist common desktop computers in a DDoS attack by loading a daemon on the local computer through an e-mail attachment.[73] According to one estimate, Trinoo networks are "being set up on hundreds, perhaps thousands, of systems that are being compromised by remote buffer overrun exploitation."[74]

After the attacker has placed the daemons on the intermediary computers, master programs are set up on other computers to act as commanders to call "the troops" into action. The attacker only needs to access the master programs, via telnet, to launch the massive, coordinated attacks.[75] Both the slave and master programs are password controlled to prevent system administrators from taking control of the Trinoo network. Once the attacker has accessed the master, he only needs to enter the IP address of the targeted server in a "dos IP" command to wake up the daemon "zombies" that begin launching their massive queries at the target. The attacker is also able to launch attacks against multiple targets using the "mdos" command.[76] Finally, the attacker can set a time limit for the DoS attack.[77]

b. Tribe Flood Network (August 1999)

Tribe Flood Network, (TFN), is a DDoS program written by a

[71] *See* Bruce V. Bigelow, *Net's Newest Pains Most Likely Caused by Feuding Hackers,* SAN DIEGO UNION-TRIB., Feb. 10, 2000, *available in* 1999 WL 29194212.

[72] *See* John Borland, *New Attack Software Released; Web Sites Now Easier Targets For Hackers,* SEATTLE-POST INTELLIGENCER, Feb. 24, 2000, at E2, *available in* 2000 WL 5289421.

[73] *See* John Borland, *Hackers Spread Simpler Tools for Vandals,* CANBERRA TIMES, Feb. 28, 2000, at A13.

[74] David Dittrich, *The DoS Project's "Trinoo" Distributed Denial of Service Attack Tool,* (Oct. 29, 1999) <http://www.ussrback.com/docs/distributed/trinoo.analysis.txt> [hereinafter Dittrich, *DoS Project*]. "A buffer overrun is when a program allocates a block of memory of a certain length and then tries to stuff too much data into the buffer, with the extra overflowing and overwriting possibly critical information crucial to the normal execution of the program." *Exploiting Windows NT 4 Buffer Overruns A Case Study, RASMAN.EXE* (visited Mar. 17, 2000) <http://newdata.box.sk/neworder/ntbufferoverruns.txt>.

[75] *See* Dittrich, *DoS Project, supra* note 74.

[76] *See id.*

[77] *See id.*

German hacker that is capable of launching ICMP, SYN Flood, UDP Flood and Smurf attacks.[78] In late August, 1999, DDoS attackers began to shift from Trinoo to TFN. Using TFN, a single attacker can launch an attack from dozens of computers on which the attacker has surreptitiously placed the TFN daemon.[79] The attacker remotely controls the TFN client network using a variety of connection methods, including telnet TCP connections.[80] Unlike various versions of Trinoo, TFN clients do not require a password to be activated, although the client sends commands to the daemon in an ICMP packet. However, there is no telnet TCP or UDP-based communication between the client and the daemon, making detection of the client's call to action more difficult to detect on the client, or master, system.[81]

c. Tribe Floodnet 2k (January 2000)

Tribe Floodnet 2k (TFN2K) is an updated version of the TFN DDoS attack tool. According to Mixter, the German hacker who wrote the program, TFN2K still contains the popular features of the original TFN, including the client/server functionality, stealth, and encryption techniques. However, Mixter added several new features that make the system more robust and deadly, including remote one-way command instructions to the distributed servers who go on to launch the attacks. Also, TFN2K boasts stronger encryption between the client and the server.[82]

[78] *See* David Dittrich, *The "Tribe Flood Network" Distributed Denial of Service Attack Tool*, (Oct. 21, 1999) <http://www.ussrback.com/docs/distributed/tfn.analysis.txt > [hereinafter Dittrich, *Tribe Flood Network*].

[79] *See Anatomy of an Attack*, THE ECONOMIST, Feb. 19, 2000, at 80, 81.

[80] *See* Dittrich, *Tribe Flood Network*, *supra* note 78. Once the hacker has placed the software on several client computers, the hacker needs to give commands to the client machines to call them into battle. This is done through a variety of connection methods, including common telnet connections. The client machines control the daemons who launch the attacks against the final targets. The hacker can be thought of as a general in the Pentagon and the clients are the field commanders orchestrating the combat units in an assault.

[81] According to the *readme.txt* that is downloaded with the TFN program, the system is easy to operate: "Usage: Install the server 'td' on a number of hosts. Put all IP addresses of the hosts running the server into a list; this will be your iplist. Run the client." *Id.*

[82] As an example of this type of attack, consider the following: If the attacker, using computer A, wanted to launch a DDoS assault on Computer F, then he would install "servers" on Computers B, C and D. Computer A can give instructions to B, C and D by randomly choosing to send the command on TCP, UDP or ICMP protocols. The internal values, or the packet's "identification papers," are optimized by the software so there is no identifiable pattern to the packets that would otherwise cause a server or router's filtering method to reject it. Then the TFN servers that were placed on Computers B, C and D decode the message that contains Computer A's spoofed, or false identification papers and begin launching an attack against

d. Stacheldraht (October 1999)

The most recent advance in DDoS attacks has come in the form of Stacheldraht, a German word for "Barbed Wire." Stacheldraht has the ability to automatically update the daemon programs, reducing the attacker's risk of intrusion.[83] Stacheldraht was based on the source code from Tribe Flood Network, with at least two significant new features. The communication between the attacker and the Stacheldraht masters are encrypted and the daemons can be automatically updated by the masters. One of the weaknesses of TFN was the attacker's connection to the master program located on the remote computers.

Stacheldraht combines Trinoo's master/daemon control features with TFN's ICMP flood, SYN flood, UDP flood, and Smurf attacks.[84] The attackers control the master computers through encrypted clients, and each master can control up to 1000 daemons that are installed on innocent third-party computers.[85] The attack begins in the preparation stage, called the "mass-intrusion phase," where large numbers of computers are compromised.[86] The attacker places the Stacheldraht daemons on the compromised systems and the daemons lie in wait for the command to attack. The third-party computers are also victims in these attacks because the systems have been compromised and they use up bandwidth and processing power.

6. Tracking Down the Attackers

The Federal Bureau of Investigation (FBI) has had a very difficult time locating the origin of the attackers because of the networked nature of the Internet, the spoofing of the DoS packets, and the procedural difficulty of organizing an investigation that involves countless jurisdictions. One method used to track the attacker is to start from the targeted server and locate the immediate server that sent the packet.[87] However, because the packet was carrying "false

Computer F. In order to further trip up egress filtering, custom IP addresses may be used to defeat the spoof filtering defense. Also, the program allows decoy packets to be sent out to Computers G to Z to hide the real location of Computers B, C and D that contain the TFN servers.

[83] *See Anatomy of an Attack, supra* note 79 at 81.

[84] *See* Dave Dittrich, *The "stacheldraht" distributed denial of service attack tool* (Dec. 31, 1999) <http://www.ussrback.com/docs/distributed/stacheldraht.analysis> [hereinafter Dittrich, *Stacheldraht*].

[85] *See id.*

[86] *See id.*

[87] *See* Martin, *supra* note 70.

identification," each subsequent router along the network could lead the investigator astray.[88]

Because the packet's "false papers" hide the true origin of the packet, it is difficult to reconstruct the origin of the spoofed packets after the fact. In order to determine where the packet came from, the investigators must set up a filer, or "trace and trap," before they arrive at that particular router. This is complicated by fact that the packet could cross as many as thirty different routers owned by ten different companies in several different legal jurisdictions.[89] In the February, 2000 attacks on the major Internet sites, the authorities have identified several university computers that were compromised and used to attack the targeted servers.[90]

The actual technique of spoofing can be complicated. For example, a traditional method of spoofing was to initiate a DoS attack on Computer B, the computer that one eventually wants to spoof. When Computer B is overwhelmed, it is not able to respond to requests from Computer C that it is requesting ACKs, or confirmation—trying to confirm they are who they said they are. The TCP tags each datagram with a sequential number. If Computer C receives a packet that is out of sequence, it will discard the packet or hold, depending on how close the packet is to the number it is looking for. The hacker, using Computer A, estimates the number that Computer C is looking for and pretends to be sending packets from Computer B by using Computer B's information or identification. Computer B is unable to stop this use of his identification because he is spending all of his time answering the false packets from another

[88] Mixter, the German hacker who authored Tribe Flood Network, comments that "[i]t will be virtually impossible to track the attackers down.... Every provider would have to scrutinize their router logs tracing back traffic to its point of origin, and that's a time-intensive process and an enormous undertaking." Iain S. Bruce, *The Hack Pack*, SUNDAY HERALD, Feb. 13, 2000, *available in* 2000 WL 4100421.

[89] *See "Trap and Trace" Authority on the Internet Urged by DOJ, FBI*, COMM. DAILY, Mar. 2, 2000, *available in* 2000 WL 4694585 [hereinafter *Trap and Trace*].

[90] According to the Department of Justice, the federal trap and trace statutes (18 U.S.C. §§ 3121-3127 (1994)) are out-of-date with Internet investigative requirements. "Pen registers" that record dialed telephone numbers and the trap and trace devices that capture incoming electronic packets to identify their origin, are not specifically covered by the statutes. Rather, the statute refers to a "device" that is "attached" to a telephone "line." *See* 18 U.S.C.A. § 3127(3) (1994). However, traffic on the Internet is not traced by telephone number, but rather by IP addresses and other information wrapped inside the packets. Also, telephone companies no longer physically connect devices to lines to route calls and Internet traffic. Instead, calls and traffic are routed by a series of electronic switches, often without wires. *See* Department of Justice, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet - A Report of the President's Working Group on Unlawful Conduct on the Internet* (Mar. 2000) <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

computer that the hacker has set up to send the packets.

7. The CFAA and Denial of Service

In any criminal law analysis, the specifics of the crime will determine which statutory section can be successfully applied. For example, the exact definition of an "intrusion" can determine whether inserting a debit card into a exterior cash machine constitutes burglary. The individual characteristics of a Denial of Service attack may also change which computer crime statutes can be applied to the attack. For example, in the above TFN2K example where the attacker used Computer A to plant "servers" on Computers B, C, and D to attack Computer F, will a traditional hacking statute be applicable for the attack on Computer F? Under 18 U.S.C. § 1030(a)(5)(B) and (C), the statute prohibits "access" of a protected computer.[91] However, are these anti-hacking statutes applicable to an attacker whose intent was to "deny access" to, rather than to merely access, the computer?

The CFAA is the primary federal anti-hacking statute, and contains seven main sections. The first section, § 1030(a)(1), protects against the knowing access of government computers to obtain classified information. This section is not applicable.

The second section, § 1030(a)(2), proscribes the intentional access of a computer without, or in excess of authorization, to thereby obtain information from a financial institution, the federal government, or any protected computer involved in interstate or foreign communications—essentially any computer connected to the Internet.[92] This section is concerned with the protection of information. The point of all of the DoS attacks is not to obtain information, but rather to bring the system down.

The third section, § 1030(a)(3), is concerned with the intentional and unauthorized access of government computers or computers used by the government. In a standard DoS attack where only one computer is used to attack another, this section is unlikely to be invoked unless the attacker targeted a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States."[93] However, in a DDoS attack, there is a better chance that this section may be relevant if the attacker placed an attack daemon on a § 1030(a)(3) protected computer. Many university computers, for example, are used by the

[91] *See* 18 U.S.C.A. § 1030(a)(5)(B)-(C) (West Supp. 1999).

[92] *See* Hatcher et al., *supra* note 1, at 403.

[93] 18 U.S.C.A. § 1030(a)(3).

federal government. Even slight activity by the daemon on the university computer could "affect" the government's use of the computer.

The fourth section, § 1030(a)(4), addresses the access and fraudulent use of a protected computer and is triggered if the value of the use obtained exceeds $5,000. Congress intended this subsection to apply, for example, to use by hackers who take over a supercomputer to run a password-breaking program. The "zombie" computers who were infected by the daemon and enlisted into the attack suffered a loss of processor power and bandwidth. This subsection could be applied against the attacker for each computer the hacker enlisted in the assault. With the subsection providing for a jail term for up to five years per instance, a hacker who plants hundreds of daemons could be liable for an extensive prison sentence.

One of the critiques of this subsection is the $5,000 damage threshold. Prosecutors have found that the $5,000 damage requirement is often both difficult to establish and an impediment to investigation. It is sometimes speculative to assess $5,000 damages if the attacker only used the computer to launch attacks. In *United States v. Middleton*,[94] the defendant challenged the government's theory of calculating the $5,000 in damages to Slip.net, an Internet Service Provider (ISP). The court held that the government's theory of loss "will be that the damage caused by defendant to the Slip.net computers caused Slip.net employees to expend time to investigate, identify, and correct the damage caused by Middleton, and take other security related steps."[95] The court agreed with the government "that the time the employees expended can be fairly valued at a figure of at least their hourly wage or salary, plus the value of benefits and overhead" provided adequate explanation of the government's theory.[96]

In addition to the uncertainty concerning the factors used to calculate the $5,000, federal authorities currently have to wait for a damage assessment to determine if there is federal jurisdiction,

[94] 35 F. Supp. 2d 1189 (N.D. Cal. 1999).

[95] *Id.* at 1193.

[96] *Id*; *see also United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II*, 62 Fed. Reg. 26616 (1997), *available in* 1997 WL 243415, which states:

> In an offense involving unlawfully accessing, or exceeding authorized access to, a protected computer as defined in 18 U.S.C. § 1030(e)(2)(A) or (B) loss includes the reasonable cost to the victim of conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service.

delaying time-sensitive investigations. For example, if a DoS attack is launched on a California web site, but the attack originated in New York, was routed through a server in New Jersey, and bounced off a computer in Wisconsin on its way to California, investigators may be required to petition the court in each jurisdiction for an order to place a trace on the activity.[97] Under a new legislative proposal by Senators Charles Schumer and Jon Kyl, the federal government would unambiguously permit federal jurisdiction as soon as the attack occurs, rather than waiting for the damage assessment.[98] Also, damage estimates below $5,000 will be treated as a misdemeanor, while damage above $5,000 will still be treated as a felony. Finally, proposed legislation specifies that the costs of responding to the attack, damage assessment costs, repair to the system and lost revenue from the interruption of service will be counted toward the $5,000 damage amount.[99] Under the present statute, the damage calculation method is unclear and there has been little judicial precedent to provide guidance for allowable damage factors.[100]

The fifth section, § 1030(a)(5), is the main anti-hacking subsection. Subsection 1030(a)(5)(A) applies to whomever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[101] The DoS and DDoS attacker would be liable under this subsection both to the "zombie" systems and to the targeted systems. The attacker causes the transmission of a program on the "zombie" system and intentionally causes damage. The attacker also causes the transmission of information, the packets, and code, the datagrams that intentionally cause damage. This subsection provides serious sentencing guidelines. A first-time conviction can subject the attacker to up to five years in prison for each occurrence. According to United States Sentencing Commission, "[i]f the defendant is convicted under 18 U.S.C. Section 1030 (a)(4) or (5), the minimum guideline

[97] *See Internet Denial of Service Attacks and the Federal Response: Panel I Of A Joint Hearing Of Crime Subcomm. of the House Judiciary Comm. and the Criminal Justice Oversight Subcomm. of the Senate Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Denial of Service Attacks*] (statement of Charles E. Schumer, United States Senator, New York).

[98] *See* Office of Charles E. Schumer, *Schumer Offers Legislative Package to Combat Online Hacking* (Feb. 16, 2000) <http://www.senate.gov/~schumer/html/schumer_offers_legislative_pac.html>.

[99] *See id.*

[100] *See id.*

[101] 18 U.S.C.A. § 1030(a)(5)(A) (West Supp. 1999).

sentence, notwithstanding any other adjustment, shall be six months' imprisonment."[102]

Section 1030(a)(5)(B) prohibits unauthorized access that recklessly causes damage to a protected computer.[103] Violation of this subsection is also a felony. However, the standard of reckless disregard is below the intentional damage provided under § 1030(a)(5)(A). If the prosecutor can show that the damage was intentional, as all DoS and DDoS attacks are, then the reckless disregard is unnecessary.

Section 1030(a)(5)(C) covers negligent damage to a protected computer. There is almost no conceivable scenario where this subsection could be used. Congress intended to punish the activity of hackers who do not intend to harm the systems but accidentally cause harm to the computer in the process. To only punish intentional harm would condone hacking into systems as long as no harm was done to the system.[104] However, in DoS and DDoS attacks, there could be no other reason a person would plant a daemon on another computer, or launch a DoS attack against another computer. Perhaps it is feasible that a curious computer user would enter a large ping command for another computer without a full understanding of the consequences. However, such conduct would be more reckless than negligent.

The sixth section, § 1030(a)(6), is concerned with the unauthorized trafficking of computer passwords and is not relevant to DoS attacks. Likewise, § 1030(a)(7) covers extortion threats against computer or network owners. This subsection would only be invoked if the attacker threatened to launch a DoS attack against the victim unless the victim pays the attacker "any money or other thing of value."[105]

[102] *United States Sentencing Commission, Sentencing Guidelines for United States Courts, Part II*, 63 Fed. Reg. 602 (1998), *available in* 1998 WL 1699.

[103] 18 U.S.C.A. § 1030(a)(5)(B) (West Supp. 1999).

[104] One group of commenators suggests that:

> [S]tate and federal governments should immediately decriminalize all forms of non-malicious hacking. Non-malicious hacking should be defined as obtaining unauthorized access to a protected computer without causing intentional or reckless damage. Successful incidents of unauthorized access should be presumed by law to be non-malicious if the actor makes a good-faith effort to report the incident to the proprietor of the accessed system immediately upon obtaining access.

Lee et al., *supra* note 2, at 882-83. However, it could be argued that such a recommendation is the equivalent of de-criminalizing breaking and entering into a store with non-malicious intent if the burglars make a good faith effort to tell the owner they broke into the store. *See id.*

[105] Bruce, *supra* note 88. None of the eight major companies that were hit by the DDoS attacks in February have reported that they received extortion threats. *See id.*

8. DoS Summary

Denial of Service attacks represent a significant threat to the stability of our network infrastructure because of the inherent vulnerability in the TCP/IP 3-handshake reliable protocol. Successful prosecution of the perpetrators should raise the awareness that DoS and DDoS are very serious crimes with serious consequences. Also, system administrators are likely to collaborate in devising plans for rapid network response to thwart the source of the attacks. However, where the system administrator's carrot may be minimized damage to their systems, the stick may be potential tort liability for allowing their system to be used in an attack against another server.[106] The tort standard of negligence could be: would a "reasonably prudent system administrator" have allowed a hacker to place a DDoS daemon on his system, and "but for" his negligence, the targeted server would not have been overloaded without his contribution? If the "zombie" computers were held liable for negligent administration of their servers, this also may help secure the Internet against DDoS attacks. Finally, the CFAA provides for a civil action for those who suffer any damage or loss against someone who violates 18 U.S.C. § 1030(a). The laws are in place to address the issue. Unfortunately, the greatest impediment to prosecuting will continue to be technical difficulty of tracing the route of the attack back to the perpetrator.

B. Web Site Defacing and Malicious Interference: User Level and Root Level Hacks

There are several reasons why a hacker would seek to hack into a web site and change a web page.[107] Web site hackers range from teenage pranksters to foreign powers seeking intelligence, and everything in between. Increasingly, there is a divide between the "old school" and "new school" hackers.[108] The "old school" hackers are associated more with the "Hacker's Ethics," a text that has been available on hacking newsgroups for several years.[109] The rift

[106] *See* Eric J. Sinrod & Bill Reilly, *Lessons of DoS Attacks*, UPSIDE TODAY, (Feb. 29, 2000) <http://www.upside.com/texis/mvm/story?id=38b6dcbe0>.

[107] According to the Director of the NIPC, "[Hackers] sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes." *Cyberattack Investigation, supra* note 25.

[108] Robert Richardson, *Hackers: Devils or Saints?*, NETWORK, June 1997, at 62.

[109] According to one hacker: "True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place the you've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool

between the two schools is often referred to as the "Black Hats" against the "White Hats."[110] The "old school" hackers complain that the widespread availability of ready-to-hack software does not require the level of sophistication that hacking required ten years ago, creating more opportunities to maliciously hack into systems without an understanding of the impact. They argue that irresponsible hacking has led to a higher profile of the "hobby" and a wave of new criminal laws that punishes both non-malicious intrusions and malicious intrusions. The "new school" hackers assert that many of the "old school" hackers have "sold out" to corporations as security experts.[111]

For the purposes of our discussion, hacking techniques will be divided into three large areas based on the hacker's intent. We will primarily address damage caused by non-authorized persons, not insiders who exceed their authorization.[112] The first major section is web site defacing and malicious interference with a web site, excluding Denial of Service attacks.[113] The second major section is unauthorized access for information and financial gain.

Basic Hacking Techniques:

There are as many hacking techniques as there are hackers. One common technique that is technically not a "hacking" technique, but is nevertheless a criminal violation, is the "cookie" exploit. A cookie is simply an HTTP header that consists of a text-only string that gets entered into the "memory" of a browser. This string contains the domain, path, lifetime, and value of a variable that a web site sets. If the lifetime of this variable is longer than the time the user spends at that site, then this string is saved to file for future reference.[114] For example, when a person signs up with a password and user name on a web site, the user's identification information is placed on the user's computer in the form of a cookie. When the user revisits the web site, the web site recognizes the user so that the user does not have to re-enter identifying information. However, some older web browsers

[sic] we live in." Dissident, *supra* note 14.

[110] *See generally* Ashley Dunn, *A Haute Commodity; Hacking, Er, Vulnerability Analysis, Is Big Business*, L.A. TIMES, Aug. 1, 1998, at D1, D3.

[111] *See id.*

[112] *See* 18 U.S.C.A. § 1030(a)(1)-(4); (5)(A) (West Supp. 1999) (including both persons who exceed their authorized access, as well as persons without authorization).

[113] *See* discussion *supra* Part III.A.

[114] *See* David Whalen, *The Unofficial Cookie FAQ*, Cookie Central (visited Mar. 5, 2000) <http://www.cookiecentral.com/faq/#1.1>.

allow remote sites to retrieve cookies that were not planted by them, enabling malicious web site operators to "steal" the cookie, effectively retrieving the username and password. For example, Buysellzone.com allows registered users to place ads and have access to the various classified ad centers on their server. However, the cookie on the user's computer holds the user's name and password in text format, not encrypted, so anyone with access to the user's cookie.txt file can access the user's account.[115]

Depending upon the purpose of the intrusion, the risk level the hacker is willing to assume, the type of server, the remote and local operating systems, and countless other variables, there is a different hacking technique that can be deployed. Rather than exploring the details of several different techniques, for the purposes of gaining enough knowledge to understand the applicable provisions in 18 U.S.C. § 1030(a), it should be adequate to walk the reader through two hypothetical hacks.[116]

Regardless of whether the hacker intends to deface a web site or steal information, the ultimate technical objective is to "get root." The "root level" is also often referred to as the "god" account, where the "god" account has access to the entire system.[117] The root level provides the hacker with the same permissions and privileges as the system administrator. If the hacker can "penetrate" to the root level, he will be able to, among countless other possibilities, change passwords, access files, change web site files, re-route server traffic, and steal credit card numbers if the server is reckless enough to store unencrypted credit card numbers on its site.[118] Once the hacker "gets root," he must eliminate traces of his intrusion—his digital footprints—so the system administrator is unaware of his access.

However, not all hacks require "root access" to damage or change files on the server. Our first example is a relatively unsophisticated hack that only requires access to a user's account on

[115] Most cookies are encrypted so that the information that is collected by the company that placed it on your computer is not readable to anyone except the company who encrypted it. On the one hand, this provides a level of security that prevents others from obtaining that information. However, the computer user is also unable to know that type of information that is being collected. It is important to note that cookies are text files, and therefore can not support a virus or software code that can place malicious scripts on a individual's computer.

[116] A few other details have been changed to give the reader an overview of the process, so as not to provide a guidebook on how to actually hack a web site.

[117] *See* Appendix A.

[118] *See* David L. Gripman, *The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 169-70 (1997).

the server. We will refer to this as a "user-level hack." The second example demonstrates a "root access" hack that is significantly more dangerous to the integrity of the machine, although the statutes do not make the distinction. According to 18 U.S.C. § 1030(a), "access" is not defined by the level of penetration. Breaching the system in any manner to obtain information, obtain something of value or cause damage is enough to trigger the statutory liability. For the terms of this paper, we will refer to this type of hack as a "root access hack."

One way to explain the difference between the two hacks is to compare them to a non-technical example—a hotel. On "hosted" web sites, where the user "rents" web space on another company's server, there are two different levels of access: that of the system administrator and that of the lessee. In a hotel, there are also two main levels of access: the hotel management and the hotel guest. A guest only has a key to access a room (user access), while management has keys to access all of the rooms, as well as the back office, front door and the storeroom (system administrator's root access). A hacker who is able to "get root" has access to the management's keys, thereby gaining full access to everything in the hotel. However, just because someone has the hotel's "all access" key, does not necessarily mean they can enter the restricted areas freely because there are security guards (system administrators) and security cameras (server access logs). The goal of the "root hacker" is to enter unnoticed, compromise the security, and depart the scene without leaving any traces of his visit.

1. Example of a User-level Hack

Hacker wants to access a computer to deface a web site that was developed using Microsoft FrontPage. Hacker employs a technique that exploits a "bug" in FrontPage web sites that use FrontPage server extensions.[119] The first thing that Hacker must address is how to prevent his access from being traced. There are many ways to hide

[119] For example:

> The FrontPage Server Extensions are a set of programs on a Web server that let the [webmaster] administer, author, and browse a FrontPage-based Web—a structure containing all of the pages, images, subdirectories, and other files that make up a Web site.
>
> The Server Extensions use standard Web server extensions interfaces, such as CGI and ISAPI, and work with virtually all existing Web servers. This design allows the FrontPage Server Extensions to be ported easily to all popular hardware and software platforms for cross-platform, Web-server compatibility.

Configuring and Deploying Microsoft FrontPage 2000 Server Extensions, (Oct. 1998) <http://www.microsoft.com/technet/FrontPg/TechNote/fpserext.asp>.

the origination of the hack, such as spoofing.[120] In this case, because Hacker does not want the victim to be able to trace him back to his point of origin, Hacker uses a laptop computer and a converted telephone lineman's handset to tap into the outside box of a neighbor's house by connecting two alligator clips to the appropriate box terminals. Hacker conducts the attack in the daytime, when the owner of the phone is not home, and the network traffic on the target site is more active.[121]

The next objective is to ascertain the user name and password for the site's webmaster, or the lessee, so he can access the web files on the server.[122] Hacker dials into a free ISP located in another region of the country to complicate the multi-company tracing investigation. Once he is on-line, Hacker enters an exploitative URL address that contains the "service.pwd."[123] Most web sites that use FrontPage server extensions locate the service.pwd in a predictable directory. If the server administrator was careless in setting up the "chmod" command that tells the server who can do what in a directory, such as granting the owner, groups or the public to read, write and execute files within the directory, then Hacker will be able to read a string of text that looks like the following: "kathy:paB.1Mg4MB6MF."[124] Hacker can already determine that the webmaster's username is "kathy." Now all that Hacker has to do is add a few commands to the password string, insert the password string into a DES decrypting password cracker and viola, Hacker has the webmaster's password as well.[125] From there, Hacker downloads the web page he wants to deface, alters the web page with his favorite web editor, and uploads the file to the server and the web page is "owned."

Applicable Federal Criminal Statutes:

In the above scenario, Hacker has broken numerous laws. Hacker would be liable under 18 U.S.C. § 1029(a)(7) which prohibits

[120] *See* discussion *supra* Part III.A.6.

[121] However, he could also attack at night when the system administrator is more unlikely to be monitoring the site.

[122] Web hosting companies provide space on their server for individuals and companies who wish to have a presence on the internet without the need to maintain their own servers.

[123] An "exploitive URL" is a URL that contains a certain string of letters and numbers that instruct the receiving server to respond in an unauthorized manner.

[124] All UNIX and Linux directories have an access level control called the CHMOD that determines the access level of different groups.

[125] Data Encryption Standard (DES) is a relatively weak encryption technique that is often used to encrypt passwords on a system.

the knowing possession of a "telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services" with the intent to defraud.[126] Hacker modified the modem and the lineman's handset, also known as a "beige box."[127] Also, Hacker may be liable for a violation of 18 U.S.C. § 1343, which prohibits the intentional scheming to obtain "money or property by means of false or fraudulent pretenses" by "wire."[128] In *United States v. Freeman*,[129] the court held that the use of a "blue box" to bypass long distance charges is a taking of property under § 1343. Hacker intentionally schemed to take "property" from the phone company or the victim whose phone line he tapped with the telephone lineman's handset. A violation of the subsection carries a prison term of not more than five years.[130]

One of the difficulties prosecutors face with many of the subsections under § 1030(a) is the requirement for "damage," which is defined as a loss aggregating at least $5,000 in value during a one year period.[131] If only the text of a web page is altered in the attack, and the system is not "damaged," then meeting the $5,000 threshold may be difficult. The subsections that penalize only the "access" with no damage requirement, § 1030(a)(1)-(3), have an easier burden to meet. However, unless the hacker has broken into a computer that contains restricted data;[132] has received information valued at more than $5,000;[133] committed acts in the furtherance of another criminal

[126] 18 U.S.C.A. § 1029(a)(7) (West Supp. 1999).

[127] According to the Jargon Dictionary, "phreaking" is the:

> [A]rt and science of cracking the phone network (so as, for example, to make free long-distance calls)....
>
> ... There was significant crossover between the hacker community and the hard-core phone phreaks who ran semi-underground networks of their own through such media as the legendary "TAP Newsletter." This ethos began to break down in the mid-1980s as wider dissemination of the techniques put them in the hands of less responsible phreaks. Around the same time, changes in the phone network made old-style technical ingenuity less effective as a way of hacking it, so phreaking came to depend more on overtly criminal acts such as stealing phone-card numbers....

The Jargon Dictionary (visited Mar. 9, 2000) <http://www.netmeg.net/jargon/terms/p.html#phreaking>.

[128] 18 U.S.C § 1343 (1994).

[129] 524 F.2d 337 (7th Cir. 1975).

[130] *See* 18 U.S.C § 1343 (1994).

[131] *See* 18 U.S.C.A. § 1030(e)(8)(A) (West Supp. 1999).

[132] *See id.* § 1030(a)(1).

[133] *See id.* § 1030(c)(2)(B)(iii).

or tortious act;[134] or committed acts for commercial or private financial gain,[135] the crime is only a misdemeanor. The three subsections that measure a threshold value of at least $5,000 for information, anything of value, or damage, are often difficult to prove in the type of hack explained above.[136]

If the web site that Hacker altered was located on a computer that is used by or for the government of the United States, then he could be liable for a misdemeanor violation of 18 U.S.C. § 1030(a)(3), which criminalizes the intentional access of such non-public computers.[137]

Hacker could be charged with a misdemeanor violation of 18 U.S.C. § 1030(a)(2)(C), which protects any information intentionally obtained from a protected computer. The "information" he obtained would be the web site owner's user name and password, along with any other information he may have viewed. The courts have held that "accessing" of information is not limited to taking the information. "Access" applies to the "intent" to access, not the "intent" to damage the protected computer.[138] Viewing the information on the computer is considered "access." In other words, the *mens rea* for this crime is the intent to access the computer and there is no requirement for the actual transport of the information. Also, if Hacker defaced the web site with a "url redirect" to his own company's web site, then the charge could be bumped up to a felony for those acts considered for commercial advantage or private financial gain.[139]

Prosecutors may be able to charge Hacker with a violation of 18 U.S.C. § 1030(a)(4) if they can show he obtained something of value worth more than $5,000 or § 1030(a)(5) if they can show Hacker caused $5,000 or more damage.[140]

[134] *See id.* at (ii).

[135] *See id.* at (i).

[136] Section 1030(a)(4) uses a $5,000 damage threshold. Section 1030(a)(2) violations are misdemeanors unless the access was for personal gain, the value exceeded $5,000, or they were committed in furtherance of another crime.

[137] *See* 18 U.S.C.A. § 1030(a)(3) (West Supp. 1999).

[138] *See* United States v. Sablan, 92 F.3d 865, 867 (9th Cir. 1996).

[139] *See* 18 U.S.C.A. § 1030(c)(2)(B)(i) (West Supp. 1999).

[140] Please note that Hacker would still be liable for any state anti-hacking statutes even if the federal government was unable to meet the statutory threshold for Federal jurisdiction. However, a discussion of state statutes is beyond the scope of this article. The definition of "damage" under 18 U.S.C. § 1030 (in addition to the $5,000 threshold), includes any impairment to the integrity of a protected computer that modifies or impairs the medical examination, diagnosis or care of one or more individuals, *see* 18 U.S.C.A. § 1030(e)(8)(B) (West Supp. 1999); causes physical injury to any person, *see id.* at (C); or threatens public health or safety, *see id.* at (D). In this scenario, none of these other definitions of "damage" are

Under § 1030(a)(4), merely viewing the information may not meet the statute's definition of "obtaining" information.[141] Congress intended to punish the theft of information, not merely punish unauthorized access.[142] In *United States v. Czubinski*, an Internal Revenue Service employee was charged with the unauthorized access of confidential income tax records. However, the court found that he only viewed the information and did not use the information in any manner. The First Circuit Court of Appeals held that the information obtained "is the showing of some additional end—to which the unauthorized access is a means—that is lacking here."[143] However, in Hacker's case, he did use the user information he obtained as a means to the additional end of hacking the web site.

2. Example of a "Root-Access" Hack

The objective of this hack is to obtain a higher system privilege than in a user-level attack, or in other words, to get the manager's "all access" keys. The first part of the hack entails getting access to the password files. The second part is cracking the password or taking advantage of a server "bug" that will allow access to the more privileged "root" level. Once at the "root" level, the hacking goal can be achieved, whether it is planting a Trojan,[144] obtaining sensitive files, downloading the system password files, stealing stored unencrypted credit card numbers, etc. The third part of the hack is covering the intrusion tracks and installing a "backdoor" that will allow future access. In this part, the system logs are modified to remove traces of the attack. Once these three steps have been achieved, the hacker is considered to "own" the system.

Hacker targets a system he wants to "own," a small business ISP that offers web site space on its server. On the ISP's system is a small company web site that sells products over the Internet and stores credit card information on the web site in a weakly encrypted form. Hacker also wants to plant a Tribe Flood Network daemon on the site.[145]

The first thing Hacker does is to sign on for a trial "shell"[146]

likely.

[141] *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997).

[142] *See id.*

[143] *Id.*

[144] *See* discussion *infra* Part III.C.3.

[145] *See* discussion *supra* Part III.A.5.b.

[146] *See* Appendix A.

account under an assumed identity with the ISP. With shell access, Hacker telnets into his shell account and enters a series of commands that exploit a "Sendmail" program.[147] Due to the "hole" in the Sendmail program, the telnet commands write a message directly to the "/etc/passwd" directory that gives Hacker a password-free root account. However, this exploit could leave several traces and may not grant him the complete access he needs to steal the credit cards, although he should be able to plant the daemon. Once he has root access, his next objective is to download the system's passwords so he can log on as another user, reducing his chances of being caught.

After Hacker has downloaded the systems passwords, he has to decipher them. After a user has created a password, the password is scrambled in an algorithm to generate a "one-way hash."[148] This requires extensive computer processing power. Many password crackers hack into more power computers to run the cracking programs. Congress specifically intended to apply 18 U.S.C. § 1030(4) to the use of another's computer processing power. Senator Jon Kyl noted during Senate discussion of the National Information Infrastructure Protection Act of 1996 that the bill:

> [A]mends 18 U.S.C. § 1030(a)(4) to ensure that felony-level sanctions apply when unauthorized use, or use in excess of authorization, is significant. Hackers, for example, have broken into computers only for the purpose of using their processing programs, sometimes amassing computer time worth far more than $5,000. The bill would penalize those whose trespassing, in which only computer use is obtained, amounts to greater than $5,000 during any one year period. Companies should not be stuck with the bill for electronic joyriders. Although they may not damage or

[147] Sendmail is a freeware program that many systems use to handle e-mail assignments. This exploit is for an older version of send mail and was patched several years ago. Although it is beyond the scope of the article to give specific hacking techniques, a non-specific demonstration of the process should be adequate to provide the elements for a statutory analysis. *See* United States v. Morris, 928 F.2d. 504, 506 (2nd Cir. 1991) (Robert Morris describes a Sendmail exploit as one of the methods he used to launch his worm program.).

[148] Most servers do not "decrypt" a password when a user enters a password on a site. Instead, the password is run through the algorithm to generate a one-way hash. If the hash matches the hash that is associated with the user name, then the password is valid. The passwords that Hacker downloaded were really just "hashes." Hacker must run the passwords through a password "cracker," which is a program that runs words and number combinations through known algorithms continuously until a match with the stolen password appears. The word that generated the matching algorithm is the password. The most common password cracking techniques are Dictionary Crackers and Brute Force Crackers. A Dictionary Cracker runs a database of words through the algorithms one a time until a match is found. A Brute Force Cracker runs every possible combination of words and letters together until the password is found.

> steal information, hackers who browse through computer systems are a significant liability to businesses who must pay for a new security system, and the expensive time the hacker used.[149]

After Hacker has cracked the password, he will log into the small business' account by File Transfer Protocol (FTP), go to the directory where the credit card numbers are stored and download the files. However, his access to the directory will be logged somewhere by the system administrator. Hacker must either use his root account, or any other password to edit the log files. Hacker will try to determine if there is anyone else on the system. If the system is clear, Hacker would explore the system to find where the log files are stored and uses a "rootkit" that will automate the sweeping up of intrusion by replacing several critical files.[150] Hacker will create a "hidden" directory on the server that will enable the directory to avoid detection with a standard Linux "ls" command which shows a list of directories in a given path.[151]

Hacker will then hide the "rootkit" in the hidden directory. In addition, if Hacker wants to continue to "own" the site for future access, he can leave a "backdoor" on the system in a modified binary that will enable him to bypass the current, and possibly any future security measures.[152] In this case, Hacker will place a Trojan program in the /bin/login/ directory under a specific user name configured for telnet logins so he can re-enter the system with the minimum amount of attention. In addition, Hacker could plant a "sniffer" that will capture all network traffic, including the user names, passwords, and credit card information. The "sniffer" will log all of the activity in a file for Hacker to retrieve at a later time. After Hacker is ready to wind up his hacking intrusion, he will initiate the "Trojan binaries" to wipe the log files and log off of the system.

Applicable Federal Criminal Statutes:

In a "root access" hack, the potential for serious crime escalates because of the information that can be obtained, the damage that can be caused, and the value of data obtained. One way to analyze

[149] *National Information Infrastructure Protection Act of 1996: Hearings on S. 982,* 104th Cong. 90 (1996) [hereinafter *Hearings on S. 982*] (statement of United States Senator Jon Kyl, United States Senetor, Arizona).

[150] *See* Lance Spitzner, *They Gain Root, Know Your Enemy: III* (last modified Aug. 13, 1999) <http://www.enteract.com/~lspitz/enemy3.html>.

[151] *See id.*

[152] *See id.*

§ 1030(a) is to first look at the type of computer that was targeted. If the computer was a federal government computer or a computer used by or for the federal government, then § 1030(a)(1)-(3) could apply. However, in the example above, Hacker most likely targeted a private ISP computer. The next step in the analysis is to determine if the hacker obtained information,[153] obtained anything more than $5,000 in value,[154] or damaged the protected computer.[155] At the point when Hacker exploited a hole in the Sendmail program, he did not obtain any information, nor did he arguably obtain anything of value, or do over $5,000 damage to the computer at this point.

However, Hacker's next move, downloading the password files, is clearly obtaining information under 18 U.S.C. § 1030(a)(2)(C) and Hacker is liable for a misdemeanor unless the prosecution can show that the value exceeds $5,000, was for personal gain, or was committed in furtherance of another crime.[156] Section 1030(a)(2)(3) was meant to protect privacy where the value of the information, although lacking quantifiable monetary value, is nevertheless valuable in terms of privacy. Also, during congressional hearings on the CFAA, Senator Leahy noted that if:

> [T]he information obtained is of minimal value, the penalty is only a misdemeanor. If, on the other hand, the offense is committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000, the penalty is a felony."[157]

If Hacker downloaded an entire batch of passwords, the prosecution may be able to argue that the aggregate value of the web site's security was more than $5,000, triggering § 1030(a)(4) liability.

Hacker's theft and possession of the credit card numbers is a violation of several statutes. First, Hacker could be liable under 15 U.S.C. § 1644(b), which proscribes the transport of stolen credit cards. In *United States v. Callihan*,[158] the court held that the defendant did not "transport" the credit card when he gave the credit

[153] 18 U.S.C.A. § 1030(a)(2)(C) (West Supp. 1999).

[154] *See id.* § 1030(a)(4).

[155] *See id.* at (5).

[156] *See id.* § 1030(c)(2)(B).

[157] *Hearings on S. 982, supra* note 149 (statement of Patrick Leahy, United States Senator, Vermont).

[158] 666 F.2d 422, 424 (9th Cir. 1982).

card number over the phone. The court concluded that the numbers by themselves did not meet the statutory language of "credit card," which "as used in section 1644 means the small, flat tablet upon which a credit card account number is imprinted, but does not mean that number alone."[159] However, a year later, in *United States v. Bice-Bey*,[160] another court held that an individual who orders goods with a fictitious name by telephone, using credit card numbers without the authorization of card holders, although she did not have cards in her possession, nevertheless violated 15 U.S.C. § 1644(a), since a core element of a credit card is the number, which can be used over telephone without seller ever seeing the plastic card itself. Although the *Bice-Bey* decision concerned the "use" of the credit card, the court still held that the credit card numbers transferred over the phone constituted a violation of § 1644(a).

Also, Hacker most likely violated 18 U.S.C. § 1029(a)(3) if he obtained more than fifteen credit card numbers.[161] Section 1029(a)(3) states that it is a punishable offense to "knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices."[162]

According to 18 U.S.C. § 1029(e)(1), an "access device" means:

> [A]ny card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.[163]

If Hacker uses one of the credit cards, he will have violated 18 U.S.C. § 1029(a)(2), if he "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value

[159] *Id.*

[160] 701 F.2d 1086, 1092 (4th Cir. 1983).

[161] In 1997, Carlos Salgado hacked into several companies and ISPs by using a packet sniffer that collected user log on information. Mr. Salgado obtained a list of thousands of credit cards and was caught when he attempted to sell them on a CD-ROM to an undercover FBI agent at the San Francisco International Airport. He subsequently pleaded guilty to four counts: two counts of computer crime under 18 U.S.C. § 1030, and two counts of trafficking in stolen credit cards under 18 U.S.C. § 1029. *See* Richard Power & Rik Farrow, *Electronic Commerce Crime; Includes Related Article on Excerpt from a Hacker's E-mail; Internet/Web/Online Service Information*, NETWORK, Dec. 1997.

[162] 18 U.S.C.A. § 1029(a)(3) (West Supp. 1999).

[163] *Id.* § 1030(e)(1).

aggregating $ 1,000 or more during that period."[164] If Hacker is found guilty of violating § 1029(a)(2) or (3), he can be sent to prison for up to ten years.[165]

When Hacker edited the log files to cover his intrusion, he caused damage to the computer under 18 U.S.C. § 1030(a)(5)(C), which criminalizes the intentional damage of a computer. His alteration of the log files resulted in reckless or negligent damage, as provided for under § 1030(a)(5)((B)-(C)). Hacker also violated the same subsection when he created a hidden directory and planted the backdoor. When Hacker installed the sniffer to intercept the network traffic, he damaged the system in violation of § 1030(a)(5)(A), possibly violated § 1030(a)(4) if he obtained anything of value from the "eavesdropping," and most likely violated § 1030 (a)(3)(C) by obtaining information from a protected computer and violated the privacy that Congress specifically intended to protect.[166]

As one can see from the above hacking examples, the hacking technique used in an attack will determine which of the subsections are relevant for both criminal and civil actions.[167]

C. *Malicious Code - Viruses, Worms, and Trojans*

Malicious code is computer code that is written with the sole intent to cause damage to a machine or to invade the machine to steal information. The most common forms of malicious code are viruses, worms, and Trojan programs. Some of these forms may share similar techniques or objectives. However, there are substantial differences between the various forms and different federal laws may apply to each form, depending on the technical method in which the offending code damages the victim.

1. Viruses

Viruses have become a serious financial and security threat to computer networks across the world.[168] According to CERT, there are an estimated 30,000 computer viruses in existence today and there are

[164] *See* 18 U.S.C.A. § 1029(c)(1)(A)(i), § 1029(a)(2) (West Supp. 1999).

[165] *See id.* § 1029(c)(1)(A)(i).

[166] *Hearings on S. 982, supra* note 149.

[167] Incidentally, 18 U.S.C.A. § 1030(g) (West Supp. 1999) allows a victim to maintain a civil action against the violator to obtain compensatory or other equitable relief.

[168] *See The Melissa Virus: Hearing of the Technology Subcomm. of the House Science Comm.*, 106th Cong. (1999) [*hereinafter Melissa Virus Hearings*] (statement of Michael A. Vatis, Director, NIPC, Federal Bureau of Investigation).

approximately 300 new viruses created each month.[169]

A virus is a program than infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness.[170] Not all viruses cause damage to its host. Viruses that are "benign," or non-harmful, are still considered viruses. For example, a virus could display an innocuous message on a certain date. Although it might be annoying and create a sense of anxiousness, the virus does not cause any measurable harm. However, the current anti-virus and anti-hacking statutes[171] do not always distinguish between harmful and benign viruses.[172]

A virus is typically spread from one computer (computer A) to another (computer B) by e-mail or an infected disk. However, the virus on computer B does not infect the computer until the program is "executed." A common method of virus execution is when computer B's user is tricked into opening a file attached to an e-mail, thinking the file is a harmless program coming from a friendly source. However, recent viruses, such as Bubbleboy, can infect a computer when a user merely reads an e-mail, without opening any attachments.[173]

A virus can also be executed by hiding a "macro" routine in a

[169] *See id.* The CERT Coordination Center is part of the Survivable Systems Initiative at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. CERT was started by DARPA (the Defense Applied Research Projects Agency, part of the U.S. Department of Defense) in December 1988 after the Morris Worm incident crippled approximately 10% of all computers connected to the Internet.

[170] *See Introduction to Computer Viruses*, Sophos Virus Info (May 26, 1998) <http://www.sophos.com/virusinfo/articles/virusintro.html>.

[171] 18 U.S.C.A. § 1030 (West Supp. 1999).

[172] *See* 18 U.S.C.A. § 1030(a)(4)-(5) (West Supp. 1999) (stating that a virus must cause "damage,"or the hacker must obtain "something of value").

[173] According to Symantec:

> VBS.BubbleBoy is a worm that works under Windows 98 and Windows 2000. The worm will also work under Windows 95 only if the Windows Scripting Host is installed. The worm will only work with the English and Spanish versions of the operating systems, and not with Windows NT. Microsoft Outlook (or Express) with Internet Explorer 5 must be used in order for the worm to propagate. The worm utilizes a known security hole in Microsoft Outlook/IE5 to insert a script file, *UPDATE.HTA*, when the email is viewed. It is not necessary to detach and run an attachment. *UPDATE.HTA* is placed in Program-StartUp of the Start menu. Therefore, the infection routine is not executed until the next time you start your computer.

Symantec AntiVirus Research Center, *VBS.BubbleBoy* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/venc/data/vbs.bubbleboy.html> [hereinafter *VBS.BubbleBoy*].

common Microsoft Office product file, like Word or Excel, and the macro can command the computer to act in harmful ways.[174] Files that contain only data, such as image files (.gif and .jpg), music files (.wav and .mp3) and text files that do not contain macro functionality (.txt) are not capable of transmitting a virus because they cannot command the computer to perform any functions.[175]

Once a virus is activated, it does not have to cause damage immediately. There are countless creative ways a virus can be triggered.[176] Most viruses contain a "payload," which contains the damaging code.[177] The "payload" is the damage a virus creates.[178] In the past, virus payloads have been triggered on a certain date,[179] when the computer re-starts,[180] or after a certain amount of times the virus is loaded into the system.[181] Viruses can hide in several places in a computer's memory.[182] Other viruses hide in computer programs so that the virus is activated every time the program is loaded.[183] Once the virus is activated, it can duplicate and spread itself without any further input by the user.[184]

Once a virus is loaded onto the hard drive[185] and "launches" its

[174] *See* Richard Raysman & Peter Brown, *Viruses, Worms, and Other Destructive Forces*, N.Y.L.J., July 13, 1999.

[175] *See id.*

[176] For example, a virus payload can be triggered to cause damage to a machine on a certain date; by launching an infected executable file; by running a companion program; or after the user enters a certain word in a program. *See id.*

[177] *See id.*

[178] *See id.*

[179] *See* Symantec AntiVirus Research Center, *W95.LoveSong.998* (visited Mar. 4, 2000) <http://www.symantec.com/avcenter/vinfodb.html> [hereinafter *W95.LoveSong.998*].

[180] *See VBS.BubbleBoy, supra* note 173.

[181] *Id.*

[182] *See* Raysman & Brown, *supra* note 174.

[183] *See id.*

[184] *See id.*

[185] A hard disk, or memory, is the main memory where programs and the operating system are permanently stored. As an example, one can think of the hard drive as a large filing cabinet, the random access memory (RAM) as a table, and the processor as a clerk. When the clerk wants to work on a file, he goes to the filing cabinet and brings the file to the table, where he can open up the file and read it. If the clerk wants to read another file, he repeats the process. The relationship between the hard drive, RAM, and processor can be further illustrated by adjusting the variables. If a lot more filing cabinets are added, but the size of the desk is still the same, the clerk will not be able to increase the number of files he can put on the table. If the size of the desk is increased, but the clerk moves slowly, then too many files on the desk may actually slow him down. The operating system is the set of instructions that coordinate all of the actions that take place in the computer. Although operating systems often come on CD-ROMs, they are not "computer programs." A program can only run "on top of an operating system." The operating system is like the translator that gets all of the hardware and software talking

payload, the results can range from annoyingly humorous like "W95.LoveSong.998," which causes a Korean love song to play on a certain date[186] to total devastation like "the Emperor," which will permanently overwrite data on the hard disk and then attempt to destroy the Flash BIOS.[187] There is also concern that a macro virus placed on a government computer could e-mail sensitive or classified material to others without the knowledge of the computer's user.[188]

a. The Melissa Virus

The Melissa Macro Virus was launched in March, 1999 and rapidly spread through computers across the world. The Melissa Macro Virus was a virus that was hidden in a Microsoft Word attachment that appeared to come from a person known to the recipient. When the attachment was opened, a list of pornographic web site passwords were displayed. However, unknown to the user, the program also activated a macro that read the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses with the message subject header "Important Message from (the name of someone on the list)."[189] The virus was estimated to have caused $80 million in damages and spread so quickly that within 48 hours, Microsoft and Intel were forced to shut down their servers.[190] One company reported that its "500-employee computer network was buffeted by 32,000 e-mail messages in a 45 minute period, effectively shutting it down for

together. In the above example, the operating system is like the employee handbook that tells the clerk what he is supposed to do and how he is supposed to do it. Many viruses hide in the boot sector area of the hard disk that the operating system checks when it begins to load the operating system.

[186] *See W95.LoveSong.998, supra* note 179.

[187] *See* Symantec AntiVirus Research Center, *Emperor* (visited Apr. 9, 2000) <http://www.symantec.com/avcenter/venc/data/emperor.html> [hereinafter *Emperor*].

> A computer's basic input-output system (BIOS) is typically a read-only memory (ROM) that is programmed at the time it is manufactured with particular low-level code responsible for basic boot functions and managing persistent data such as the date and time. Most recent PCs have been manufactured with a relatively new type of memory called *Flash* ROM. BIOS in Flash ROM is often referred to as Flash BIOS. Flash BIOS capability means that enhancements can be installed using a special program without having to physically replace a chip.

Mitre (visited Mar. 31, 2000) <http://www.mitre.org/research/cots/FLASHBIOS.html>.

[188] *See Melissa Virus Hearings, supra* note 168 (statement of Michael Vatis, Director, NIPC, Federal Bureau of Investigation).

[189] Raysman & Brown, *supra* note 174.

[190] *See ZDTV Exclusive: Accused Author of Melissa Computer Virus to Plead Guilty in Court Tomorrow*, PR NEWSWIRE, Dec. 8, 1999.

legitimate purposes."[191]

The author of the virus, David Smith, was quickly caught and pled guilty to state[192] and federal charges. Mr. Smith pled guilty to intentionally causing damage to computers, 18 U.S.C. § 1030(a)(2), (5)(A), with an admission that he was responsible for the $80 million in damages that affected over a million computers.[193] The Melissa Macro Virus resulted in the first successful prosecution of a virus writer in over a decade[194] and only the second successful prosecution in history,[195] despite the fact that viruses continue to plague the Internet.[196]

Applicable Federal Criminal Statutes:

The relevant and tested federal anti-virus statutes are 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(a)(2). If a virus is loaded into a computer by an e-mail attachment, and the author intended to cause "damage" to the recipient computer, then 18 U.S.C. § 1030(a)(5)(A) is applicable. Section 1030(a)(5)(A) prohibits the knowing transmission of a program, code, or command, that results in intentional damage without authorization to a protected computer.

If the virus author did not intend to cause damage to the computer, but rather the code accidentally damaged the computer as a result of the e-mail transmission, then as an alternative to the above statute, the author may be prosecuted under 18 U.S.C. § 1030(a)(5)(B) which covers reckless damage to a computer as a result of unauthorized and intentional access. The penalties for both § 1030(a)(5)(A) and (B) are the same—up to five years in prison. A negligence standard would be considered too low for an intentional act, as provided by 18 U.S.C. § 1030(a)(5)(C), which is a misdemeanor.

If the recipient of the virus forwards the virus on to another

[191] *Melissa Virus Hearings, supra* note 168.

[192] Mr. Smith plead guilty to second-degree computer theft under N.J.S.A. 2C:20-25. *See Cyberattack Investigation, supra* note 25.

[193] *Cyberattack Investigation, supra* note 25.

[194] *Denial of Service Attacks, supra* note 97.

[195] *See id.*

[196] One of the most common viruses in 1999 and 2000 is another Microsoft Word Macro virus called WM97/Marker. *See Sophos Virus Info* (visited Mar. 14, 2000) <http://www.sophos.com/virusinfo/topten/>. This virus sends a message to an Internet site containing the File Information Summary whenever the window is closed. *See id.* Although this information may not be highly sensitive, it could only be the beginning of significant invasions of privacy on the Internet by viruses.

person via e-mail, then his mental state, or *mens rea*, will determine his culpability.[197] If he is unaware that there is a virus, then he will not have the requisite mental state.[198] If he is aware that there is a virus, then he could face § 1030(a)(5)(A) liability because he intentionally sent the virus.[199] However, if he was aware there was a virus attached to the e-mail, but he thought it was a harmless prank, for example, then his act could be reckless or negligent; mental states that can trigger § 1030(a)(5) sanctions.

There is a possibility that a virus may not reach federal jurisdiction if the virus was transmitted to a stand-alone computer by diskette. Section 1030(a)(5) covers only "protected computers," those that are "used in interstate or foreign commerce or communication."[200] If the computer has a modem or a fax server loaded on it, then the prosecution could argue that it is a protected computer because it is a computer "which is used in interstate or foreign commerce or communication."[201] However, if the virus is loaded onto a non-networked computer that, for example, is used in a small office for billing and the virus is placed on it by a diskette, a strong argument can be made that it is not a protected computer under federal jurisdiction because it is not a computer "which is used in interstate or foreign commerce or communication."[202]

However, if the virus is loaded onto a computer and causes any of the enumerated damages in § 1030(e)(8), then action against the attacker might be brought under the statute. For example, if the virus was loaded onto a computer that was used to store medical records, and if the virus impaired the treatment or care of an individual because the patient's medical records were destroyed, then it would trigger criminal liability even though the damage did not meet the monetary threshold.[203] Of course, there are state anti-virus laws which would bring the attack under state jurisdiction if federal jurisdiction is unavailable. However, a discussion of state statutes are beyond the scope of this article.

Section 1030(a)(2) has been successfully used against viruses that have invaded the system and sent information from the

[197] *See* Haeji Hong, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 296 (1997).

[198] *See id.*

[199] *See id.*

[200] 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

[201] *Id.* § 1030(e)(2)(A).

[202] *Id.*

[203] *Id.* § 1030(e)(2)(8).

computer.[204] Section 1030(a)(2)(C) criminalizes the intentional access of a computer without, or in excess of authorization, to obtain information from any protected computer if the conduct involved interstate or foreign commerce. In this case, it is irrelevant if the virus was loaded into the computer by a diskette because the e-mailing of the information, such as Melissa's fifty e-mail contacts, invokes federal jurisdiction because it involves interstate and foreign commerce.

Finally, if the e-mail attachments made their way to a Federal Government computer or a computer that "is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States," then the sender of the virus could be liable for a misdemeanor under § 1030(a)(3).[205]

If a Melissa Macro-type virus were to infect a Government computer, then the virus sender could be liable under § 1030(a)(2)(B), which prohibits the intentional access of a computer and obtaining information from the Federal Government. The e-mail addresses in Microsoft Outlook could be considered "information." However, if any information that is considered protected against unauthorized disclosure "for reasons of national defense or foreign relations, or any restricted data," then the virus sender could be liable under § 1030(a)'s most serious violation—§ 1030(a)(1). This subsection provides for a prison term up to ten years.

2. Worms

Worms are similar to viruses. However, one major distinction is that worms multiply without any human interaction. A worm can wind its way through a network system without the need to be attached to a file, unlike viruses.[206]

The Haiku worm is a good example of a robust worm with many features. The Haiku worm spreads itself through e-mail with an attachment called "haiku.exe." When the worm is executed, it modifies the system to load every time the computer is re-booted. After the computer is re-booted, a small haiku poem will appear in a window box. The worm generates it own haikus from a list of words. The worm will also search the hard drive for e-mail addresses and the worm will send haiku.exe with a message to the e-mail addressees it

[204] *See* Wendy Davis, *Prosecutors Watching the Web Street Crime is Down, but that may Just Mean it's Moving Online,* 158 N.J. L.J. 933 (1999).

[205] 18 U.S.C.A. § 1030(e)(2)(8) (West Supp. 1999).

[206] *See* Raysman & Brown, *supra* note 174.

located on the hard drive.[207] However, although the worm is annoying, it is not malicious.

a. The Morris Worm

Robert Morris was a first-year graduate student in Cornell University's computer science Ph.D. program when he released a computer worm with the intent to demonstrate the vulnerability of computers to malicious programs. He programmed the worm to multiply only once on a computer, thereby helping the worm evade detection. However, to defeat system administrators who might trick the worm into thinking the computer already had the worm, Morris designed the worm to automatically reproduce every seventh time, regardless of whether the machine already had the worm. However, Morris underestimated the number of iterations the worm would make. The worm multiplied across the Internet much more quickly than anticipated and he made attempts to limit the damage by releasing a solution over the Internet. However, due to network congestion caused by the worm, the solution was not able to get through until serious damage had already been done to many protected computers across the country. The estimated cost to repair each infected installation ranged from $200 to more than $53,000. Morris was charged with violating 18 U.S.C. § 1030(a)(5)(A). The trial court convicted Morris and the Second Circuit upheld the conviction on grounds that § 1030(a)(5)(A) "does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss."[208] In 1996, Congress codified the *Morris* court's holding by specifying the levels of *mens rea* required for three subsections of § 1030(a)(5), two felony and one misdemeanor.

Applicable Federal Criminal Laws:

As some worms multiply exponentially and wind their way through the Internet, they can cause extensive damage in overloaded servers and anti-worm extraction. If a company has 500 computers on a network that become infected, the cost to extract the worms would easily meet the $5,000 threshold for damages. As Congress

[207] Symantec AntiVirus Research Center, *W95.Haiku.16384.Worm* (visited Apr. 6, 2000) <http://www.symantec.com/region/uk/avcenter/venc/w95_haiku_16384_worm.html> [hereinafter *W95.Haiku.16384.Worm*].

[208] United States v. Morris, 928 F.2d 504, 505 (2nd Cir. 1991).

learned after the *Morris* case, the intent to access,[209] not the intent to damage, has to be the standard as the world becomes more interconnected.[210]

If a worm is received by a user and executed and installed in the system, § 1030(a)(5)(C) would cover the knowing transmission of that program if it caused an aggregate $5,000 in damage. Sections 1030(a)(5)(B)-(C) may not be available because of the non-targeted nature of worms. Those subsections proscribe the "intentional access" of protected computers and a worm is indiscriminately sent out, at least after the first wave. Likewise, nothing of value is taken[211] and no information is obtained,[212] so the other subsections will not be relevant in a standard self-replicating worm program.

3. Trojan Horse Programs

A Trojan Horse program, or Trojan program, is an innocent-looking program that contains hidden functions. They are loaded onto the computer's hard drive and executed along with the regular program. However, hidden in the belly of the "innocent" program is a sub-program that will perform a function, mostly unknown to the user. Trojan programs can take the form of a popular program where the original source code has been altered to hide the Trojan "payload."

a. Back Orifice 2000

Back Orifice 2000 (BO2K) is a Trojan program that is designed for misuse and attack on another computer. It is an advanced program that takes a group of complex hacking and networking activities and bundles them into one graphical interface. The hacker has the victim install the "server" on his computer without his knowledge, typically in the form of an e-mail attachment. After the victim has loaded the BO2K on his machine, the hacker is able to gather information on the victim's computer, perform system commands, redirect network traffic and reconfigure the victim's computer. The damage that a hacker can do to a computer is limitless, and the invasion of privacy could cause serious damage to companies and individuals. BO2K invisibly resides on the remote

[209] The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. *See id.* at 506.

[210] *See* Hatcher et al., *supra* note 1, at 406-07.

[211] 18 U.S.C.A. § 1030(a)(4) (West Supp. 1999).

[212] *See id.* at (1)-(3).

victim's computer and can perform unauthorized actions without the user's knowledge. If the victim is on a network, the hacker could gain broad access to that network.[213]

The installation of BO2K involves installing the client on the hacker's computer and getting the victim to install the server on his machine. Once BO2K has been properly configured, the server sitting on the victim's computer silently waits for instructions from the hacker's client. BO2K has over seventy commands that it can send from the hacker's client to the server. The hacker simply has to scroll down a list of commands, click on the command he wants to initiate on the remote server, and push the "Send Command" button. The server's response will appear in a window below the command list.[214] The solution to these Trojan programs is to avoid opening e-mail attachments, particularly from non-trusted sources. In addition, all of the major anti-virus detection kits can locate BO2K software on computers.

Applicable Federal Criminal Laws:

Trojan programs are specifically the type of computer crimes § 1030(a) was meant to address because the likelihood of malicious damage that can cause millions of dollars in damages is very high. As the economy becomes more inter-networked, the risks posed by programs such as BO2K are increasing.

Like virus distribution, if the Trojan program writer gives a program on a diskette to someone who installs the program on a stand-alone computer, and the computer is damaged, there may not be adequate Federal jurisdiction in this scenario. The computer may not be considered a "protected computer" that is "used in interstate or

[213] BO2K can be analogized to receiving a package that contains a hidden microphone.

[214] The following are examples of BO2K Commands: System commands, including the ability to shut down and reboot the remote computer, freeze up the remote computer and retrieve a list of the user names and passwords located on the machine; Key Logging commands enable the hacker to send each keystroke the victim makes to a text file on the victim's computer, where he can later retrieve the keystroke log file with the click of a button. Keyloggers are the most pernicious of privacy invasions because the keystroke logger saves every key pressed on the keyboard, eliminating the possibility of erasing your thoughts or later encrypting them because the hacker has access to every letter you typed before you erased the documents or encrypted it; MS Networking commands allows the hacker to access other computers on a local network; Registry commands enables the hacker to edit the computer's registry, the virtual "guts" of the computer system; Multimedia Commands permits the hacker to capture video stills and play .wav files located on the remote computer; File/Directory commands provide the hacker with the ability to view the directory list, and find, view, copy and delete files. Obviously, this type of silent access on a computer is a severe invasion of privacy. *See* BO2K Docs (visited Apr. 7, 2000) <http://www.bo2k.com/docs/cmdrefindexbar.html>.

foreign commerce or communication."[215]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" is harmless, it may be difficult to establish "damage" under § 1030(a)(4) or § 1030(a)(5). According to § 1030(e)(8), "damage" is defined as any "impairment to the integrity or availability of data, a program, a system or information that (A) causes a loss aggregating at least $5,000 in value during any 1-year period or one or more individuals."[216]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the "payload" *does* cause damage, and if the "damage" definition in § 1030(e)(8) can be met, then the program author would at least be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program, information, code, or command that intentionally causes damage. If the Trojan program makes its way onto several computers, the damage calculation could be met more easily due to § 1030(e)(8)'s damage definition that includes "one or more individuals."[217]

If the Trojan program writer e-mails a program that a recipient surreptitiously loads onto a computer, and the Trojan program is a program similar to Back Orifice that transmits information from the victim's computer to another computer, then there are several statutes that could apply to the Trojan writer's actions, depending on the computer that was infected.

If the computer infected by a BO2K-type Trojan was a private person or company, then the hacker would be liable under § 1030(a)(2), which prohibits obtaining information from the intentional unauthorized access of a protected computer. Here, there is no damage threshold. However, this crime is presently only a misdemeanor, unless the value of the information exceeds $5,000 or it was committed in the furtherance of another crime, in which case it is bumped up to a felony.

Under the same scenario, the hacker would also be liable under § 1030(a)(5)(A), which prohibits the knowing transmission of a program or command that intentionally causes damage to a protected computer. Once again, the damage threshold is an aggregate $5,000 in any one year period to one or more individuals. If this burden can

[215] 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1999).

[216] *Id.* § 1030(e)(8).

[217] *Id.*

be met, then the hacker is subject to up to five years in prison.

Theoretically, under this scenario, the Trojan program writer could be liable under § 1030(a)(4). That subsection covers the knowing intent to defraud a protected computer and the procurement of anything of value in excess of $5,000. This is a felony crime. Nonetheless, Congress did not want to make a felony out of every hacker that breaks into a computer and uses its processing power, for example, and does not obtain anything of value.[218]

The hacker could be liable under the more serious § 1030(a)(1) and subject to ten years in prison if the hacker's BO2K Trojan ends up on any computer containing information that is protected by a national statute, or restricted data that could be considered to be used to the injury of the United States, or to the advantage of any foreign nation. The delivery element is met because even if the information is not transferred to the hacker's client computer, there is a provision in the subsection for an attempted transmission.

IV. NEW COMPUTER CRIME LEGISLATION

Senators Charles Schumer and Jon Kyl have introduced new legislation, S. 2092, aimed at addressing some of the perceived weaknesses in the CFAA. The three main provisions addressed by this new legislation propose the following: trap and trace orders, federal jurisdiction requirements, and sentencing.[219]

First, the new legislation would make it easier for cyber-investigators to obtain "trap and trace" orders. "Trap and trace" devices are used to capture incoming IP packets to identify the packet's origins. Due to the ease with which hackers are able to "spoof" their true origin, the most effective way to reconstruct the path of a virus, DoS, or hacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrive at each individual router or server. In the case of a single telephone company, it has been relatively easy for investigators to obtain trap and trace orders.[220] According to Congresswoman Scott of Virginia, "one communication is being carried by several different [ISPs], by a telephone company or two, local or long distance, by a cell company or two, and soon enough by a satellite company or two."[221] Once the segment of the route goes beyond the court's

[218] *See* Hatcher et al., *supra* note 1, at 407.

[219] *See Trap and Trace*, *supra* note 89.

[220] *See id.*

[221] *Id.*

jurisdiction, investigators must then go to the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace an on-line communication from start to finish.[222]

The second provision would lower the monetary barrier for federal jurisdiction. Currently, the CFAA requires a damage threshold in excess of $5,000.[223] However, the $5,000 threshold is often difficult to establish when there is no fixed monetary value to the information. Also, investigators must currently wait for a damage assessment before they can initiate an investigation, which can cause expensive delays. The new legislation would permit federal jurisdiction at the outset of an attack. Crimes that exceed $5,000 will still be treated as felonies.[224] However, attacks that cause less than $5,000 in damage would be defined as misdemeanors. Finally, the legislation clarifies what is included in the calculation of "damage," making it easy to reach the $5,000 threshold.[225] It provides for the costs of responding to the offense, the damage assessment costs, restoration costs, and any lost revenue or costs incurred from the interruption of service.[226]

The third provision would modify the strict sentence directives contained in the Antiterrorism and Effective Death Penalty Act of 1999 which required a mandatory incarceration for a minimum of six months for any violation of 18 U.S.C. § 1030(a).[227] Some hacking crimes have gone unprosecuted because the six month sentence was considered excessive. The new legislation would provide lesser sentences for lesser crimes, helping to ensure that all levels of hacking cases will be prosecuted.[228]

Finally, the proposed legislation would make juvenile perpetrators fifteen years of age and older eligible for federal prosecution in serious computer crime cases at the Attorney General's discretion.[229]

However, the proposed changes have raised privacy concerns. A report written by the President's Working Group on Unlawful Conduct on the Internet entitled "The Electronic Frontier: the

[222] *See id.*

[223] *See* S. 2092 IS, 106th Cong. §2 (2000).

[224] *See id.*

[225] *See id.*

[226] *See id.*

[227] *See id.*

[228] *See id.*

[229] *See* S. 2092 IS, 106th Cong. §2 (2000).

Challenge of Unlawful Conduct Involving the Use of the Internet" has raised the concerns of privacy advocates.[230] The groups are particularly concerned about the potential for trap and trace abuse by authorities.[231] The American Civil Liberties Union (ACLU), would like to raise the standards for trap and trace devices, rather than lower them.[232] According to the ACLU, law enforcement currently only needs to overcome "minimum obstacles" to obtain trap and trace devices.[233] The ACLU is concerned that an expansion of the government's power to obtain trap and trace orders will enhance the government's power to "surreptitiously intercept even more personal electronic communications."[234] The current standard for a trap and trace order is that the investigator must assert in writing to the court that the information is "relevant" to an ongoing investigation.[235] According to the ACLU, the "judge to whom the application is made *must* approve the application, *even if he disagrees* with the assertions of law enforcement."[236]

Additionally, the ACLU is concerned that an expansion of the substance of the orders will erode privacy. The ACLU speculates that an expansion of the powers "might allow law enforcement agents to access a variety of data, including dial-up numbers, IP addresses, electronic mail logs, uploaded files, and so on.... without a court order."[237]

The CFAA is broad enough to cover most computer crimes. The Act protects government and private computers against inside and outside threats to information, fraud, and damage. Continued proactive legislative changes to keep the Act up to date in the escalating cyber-war between secure web sites and hackers will be critical to maintaining the integrity of our increasingly inter-networked society. One challenge in the near future will be the expansion of the number of devices that are able to access the Internet. For example, as televisions become "web-enabled," allowing users to access the

[230] Robyn E. Bumner, *Government Wants to Bore Web Peephole*, ST. PETERSBURG TIMES, Mar. 12, 2000, at 4D.

[231] *See, e.g.*, letter from Barry Steinhardt, Associate Director, ACLU, to Janet Reno, Attorney General of the United States (Mar. 8, 2000) (on file with the *Santa Clara Computer and High Technology Law Journal*).

[232] *See id.*

[233] *See id.*

[234] *Id.*

[235] *See id.*

[236] *Id.*

[237] Letter from Barry Steinhardt, *supra* note 231.

Internet from their televisions, will televisions be considered "high-speed data processing devices" as defined under the Act's "computer" definition? Would passwords taken from the television's cookie storage be protected under the Act? As Wireless Application Protocol (WAP) brings the Internet to hand-held devices and mobile telephones, will the devices and telephones be considered "protected computers"?

Cyber-crime prosecutors are also facing the difficulty of attacks that originate overseas beyond their jurisdiction. If part of a hacking trail is routed overseas, unless the U.S has an agreement with the foreign jurisdiction, that trail could lead to a dead end if investigators do not have access to the server's logs. The world of individual national jurisdictions will need to address the increasingly borderless crimes committed in cyberspace. However, the CFAA provides a solid foundation upon which we can develop new cyber-crime laws for the coming century.

V. CONCLUSION

Over the course of the past ten years, cyber-crimes have progressed from being malicious pranks by disenchanted teenagers to a serious threat that will tax the resources of crime enforcement and potentially destabilize society. Successful criminal prosecution and civil litigation will require that members of the legal community familiarize themselves with the various hacking techniques to ensure that the perpetrators are tried and convicted under the relevant statutes. A misapplication of the law to a specific hacking technique could allow a hacker to walk free. Likewise, members of the business community must understand the serious risks associated with conducting business on-line and their responsibility to the other companies for negligent maintenance of their systems.

And finally, hackers who naively believe in their right to access information, must be made aware that even harmless computer intrusions can trigger criminal sanctions. The financial stakes have risen dramatically over the past five years. Until there are more high profile hacking prosecutions, naïve hackers will continue to believe that they are invulnerable and their hacks are a form of innocent digital thrill seeking. Nevertheless, over the next few years, there will be a few hackers whose only hacking and cracking is going to be breaking rocks on a chain gang.

APPENDIX A

The following definitions are taken from the Jargon Dictionary: *The Jargon File, version 4.2.0,* available on-line at <http://www.netmeg.net/jargon/>.

cracker *n.* One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker []. An earlier attempt to establish 'worm' in this sense around 1981-82 on Usenet was largely a failure.

Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).

Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life.

Ethical considerations aside, hackers figure that anyone who can't imagine a more interesting way to play with their computers than breaking into someone else's has to be pretty losing [sic].

daemon */day'mn/ or /dee'mn/ n.* [from the mythological meaning, later rationalized as the acronym 'Disk And Execution MONitor'] A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The idea is that the perpetrator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). For example, under ITS writing a file on the LPT spooler's directory would invoke the spooling daemon, which would then print the file. The advantage is that programs wanting (in this example) files printed need neither compete for access to nor understand any idiosyncrasies of the LPT. They simply enter their implicit requests and let the daemon decide what to do with them. Daemons are usually spawned automatically by the system, and may either live forever or be regenerated at intervals.

Daemon and demon are often used interchangeably, but seem to have distinct connotations. The term 'daemon' was introduced to computing by CTSS people (who pronounced it /dee'mon/) and used it to refer to what ITS called a dragon; the prototype was a program called DAEMON that automatically made tape backups of the file system. Although the meaning and the pronunciation have drifted, we think this glossary reflects current (2000) usage.

FTP */F-T-P/, not* /fit'ip/ **1.** *[techspeak]* n. The File Transfer Protocol for transmitting files between systems on the Internet. **2.** vt. To beam a file using the File Transfer Protocol. **3.** Sometimes used as a generic even for file transfers not using FTP. "Lemme get a copy of "Wuthering Heights" ftp'd from uunet."

hacker *n.* [originally, someone who makes furniture with an axe] **1.** A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. **2.** One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. **3.** A person capable of appreciating hack value, which is defined as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. **4.** A person who is good at programming quickly. **5.** An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) **6.** An expert or enthusiast of any kind. One might be an astronomy hacker, for example. **7.** One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. **8.** *[deprecated]* A malicious meddler who tries to discover sensitive information by poking around. Hence 'password hacker', 'network hacker'. The correct term for this sense is cracker. . . .

root *n. [Unix]* **1.** The "superuser" account (with user name 'root') that ignores permission bits, user number 0 on a Unix system. The term avatar is also used. **2.** The top node of the system directory structure; historically the home directory of the root user, but probably named after the root of an (inverted) tree. **3.** By extension, the privileged system-maintenance login on any OS. . . .

server *n.* A kind of daemon that performs a service for the requester and which often runs on a computer other than the one on which the server runs. A particularly common term on the Internet, which is rife with 'web servers,' 'name servers,' 'domain servers,' 'news servers,' 'finger servers,' and the like.

shell *[orig. Multics n.* techspeak, widely propagated via Unix] **1.** *[techspeak]* The command interpreter used to pass commands to an operating system; so called because it is the part of the operating system that interfaces with the outside world. **2.** More generally, any interface program that mediates access to a special resource or server for convenience, efficiency, or security reasons; for this meaning, the usage is usually 'a shell around' whatever. This sort of program is also called a 'wrapper.' . . .

TCP/IP */T'C-P I'P/ n.* **1.** [Transmission Control Protocol/Internet Protocol] The wide-area-networking protocol that makes the Internet work, and the only one most hackers can speak the name of without laughing or retching. Unlike such allegedly 'standard' competitors such as X.25, DECnet, and the ISO 7-layer stack, TCP/IP evolved primarily by actually being *used*, rather than being handed down from on high by a vendor or a heavily-politicized standards committee. Consequently, it (a) works, (b) actually promotes cheap cross-platform connectivity, and (c) annoys the hell out of corporate and governmental empire-builders everywhere. Hackers value all three of these properties. . . .

TELNET */tel'net/ vt.* (also commonly lowercased as 'telnet') To communicate with another Internet host using the TELNET [] protocol (usually using a program of the same name). TOPS-10 people used the word IMPCOM, since that was the program name for them. Sometimes abbreviated to TN /T-N/. "I usually TN over to SAIL just to read the AP News."