Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Federal Computer Crime Laws

The Internet has been a boon to business, science, education and just about any field you can think of, including crime. Just like every human invention, Internet has two sides to it, on the one hand it allows businesses to be more productive and scientists to share research data almost instantaneously, on the other hand it grants criminals an additional tool to commit crimes and get away with it. Because of its unique nature that transcends national borders and the anonymity that it allows for its users, Internet is p...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Federal Computer Crime Laws

Maxim May
GSEC Practical 1.4b
June 1, 2004

Abstract

The Internet has been a boon to business, science, education and just about any field you can think of, including crime. Just like every human invention, Internet has two sides to it, on the one hand it allows businesses to be more productive and scientists to share research data almost instantaneously, on the other hand it grants criminals an additional tool to commit crimes and get away with it. Because of its unique nature that transcends national borders and the anonymity that it allows for its users, Internet is perfect for those who wish to evade the law. Computer related crime is an unavoidable risk that all IT professionals have to face and protect their networks against, as such it is important to know what laws are there that deal with computer related crime. In this paper I will describe the major US federal legislation that has been enacted to deal specifically with the problem of computer crime.

Computer Crimes

Internet has spawned new forms of crimes and made old crimes easier to commit, cyber-stalking, identity theft, child pornography, fraud and scams, copyright violations, hacking and creating malicious code, the list goes on and on. In a 2003 survey conducted by the CSI with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, of the 530 respondents made up of U.S. corporations, government agencies, financial institutions, medical institutions and universities, 56% reported unauthorized use of their computer systems.[1] The total financial loss amongst 251 respondents who chose to report it was $201,797,340. Of that amount the greatest portion, $70,195,900, was lost due to theft of proprietary information, the next biggest portion, $65,643,300, was lost due to denial of service attacks. The two highest methods of attack or misuse reported were virus incidents, 82%, and insider abuse of network connections, 80%. It can be seen from the above statistics that Internet is still very much a lawless place, the question is what are the authorities doing about it.

As is always the case, the laws that take into account the new and constantly evolving technologies are always lagging behind the criminals who make use of these technologies. The first law used to prosecute computer criminals in the US is the wire fraud statute[2] that prohibits the use of communication wires that are

[1] "2003 CSI/FBI Computer Crime and Security Survey", internet, http://www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm
[2] Title 18 U.S.C. § 1343, internet, http://www4.law.cornell.edu/uscode/18/1343.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

utilized in interstate or international commerce in any attempt to commit a fraud. In fact the wire fraud statute is still used to effectively prosecute computer related crimes even today. The law requires proof of some type of plan to defraud out of money or property and that interstate or international wires were used during the crime. Of course the wire fraud statute was written without computer crime in mind and as such it has serious limitations when dealing with it, not all computer related crimes can be prosecuted with it, not every crime committed using a computer is done with the intent to commit a fraud, and not all computer crimes use interstate or international wires. The problems with the traditional laws when applied to computer related crimes became clearly apparent to the authorities who began calling for new laws specifically tailored to deal with the computer related crimes.

Computer Fraud and Abuse Act

The Congress responded to the problem of computer crime by enacting several laws. The first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 ("CFAA"). The fact that only one indictment was ever made under the original CFAA before it was amended in 1986 shows how difficult it is to write effective computer crime legislation.[3] CFAA is the most important computer crime statute in the U.S. because almost every other statute that deals with computer crime modifies the CFAA.

Originally CFAA had a major limitation because it required proof that the person accessed the computer without authorization[4]. Thus by focusing on the method of entry into the computer instead of the use of the computer, the statute excluded any crimes committed by an insider, which couldn't be prosecuted under the CFAA. Another limitation of CFAA was specifically written into it, the statute forbade prosecution for access to a computer where the only thing of value gained by the intruder was the use of the computer itself.[5] As such, according to CFAA, merely viewing data stored on the computer was not illegal even if access was gained without authorization.

In 1994 Computer Fraud and Abuse Act was modified again in order to deal with the problem of "malicious code" such as viruses, worms and other programs designed to alter, damage or destroy data on a computer.[6] This was necessary because the old law only focused on access of the computer system and not on how that computer system was used. The amended CFAA could now be used to prosecute those who transmitted "a program, information, code, or command to a computer or computer system" with the intent to cause damage to the computer

[3] D. Glenn Baker, "Trespassers Will be Prosecuted: Computer Crime in the 1990's," Computer/Law Journal Vol. 12, No. 1 (Oct. 1993): 68.
[4] Computer Fraud and Abuse Act 1986 (US) 18 USC 1030, internet, http://bar.austlii.edu.au/au/other/crime/123.html
[5] Computer Fraud and Abuse Act 1986
[6] Title 18 U.S.C Section 1030, internet, http://www4.law.cornell.edu/uscode/18/1030.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

or information in the computer or prevent the use of the system without the knowledge or the authorization of the owners of that computer. In addition, the law made it a crime to act "with reckless disregard of a substantial and unjustifiable risk" of damage or loss occurring.

The National Information Infrastructure Act (NIIA) was passed in 1996 to expand the CFAA to encompass unauthorized access to a protected computer in excess of the parties' authorization.[7] This was a necessary change because before NIIA was passed, only if the criminal had acted for commercial gain could he be charged under CFAA. After NIIA was passed, it became illegal to even view information on a computer without authorization.

CFAA is also known as Title 18 U.S.C Section 1030.[8] Section 1030(a) includes in it the types of activities that CFAA protects against. In its current incarnation CFAA criminalizes seven types of computer activities: (1) the unauthorized access of a computer to obtain national security information with an intent to harm the United States or for the benefit of a foreign nation; (2) the unauthorized access of a computer to obtain protected financial or credit information; (3) the unauthorized access of a computer used by the federal government; (4) unauthorized access to a protected computer with the intent to defraud; (5) intentionally damaging a protected computer; (6) the fraudulent trafficking in computer passwords and any other information which can be used to gain access to a protected computer; and (7) threatening a protected computer with the intent of extorting money or something else of value. The term "protected computer" is defined in the CFAA as either a computer in use by a financial institution or the United States Government or a computer used in interstate or foreign commerce or communication. A more detailed listing of the Section 1030(a) can be found below.

Section 1030(a)(1) makes it illegal to access a computer without authorization or in excess of one's authorization and obtain information about national defense, foreign relations, or restricted data as defined in the Atomic Energy Act of 1954[9], which covers all data concerning design, manufacture or utilization of atomic weapons and production of nuclear material. It is worth noting that section 1030(a)(1) requires proof that the individual knowingly accessed the computer without authority or in excess of authorization for the purpose of obtaining classified or protected information. Section 1030(a)(1) criminalizes the use of a computer to gain access to the information, not the unauthorized possession of it or its transmission. U.S. laws already provide a basis for punishing individuals who steal classified information, the primary purpose of Section 1030(a)(1) is to

[7] National Information Infrastructure Protection Act of 1996, internet, http://www.epic.org/security/1996_computer_law.html
[8] Title 18 U.S.C Section 1030
[9] Atomic Energy Act of 1954, internet, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf#pagemode=bookmarks&page=14

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

punish those who break into computer systems or attempt to do so in order to obtain classified information.

Section 1030(a)(2) makes it illegal to intentionally access a computer without authorization or in excess of authorization in order to obtain records of a financial institution, or to obtain personal records of consumers from a consumer reporting agency. This section also makes it illegal to obtain information from any department or agency of the United States or any protected computer that is involved in interstate or foreign communication. Section 1030(a)(2) is a very broad section that covers a vast swath of computers, it criminalizes unauthorized access to any federal computer or any computer belonging to a financial organization. The section about the protection of computers that take part in interstate or foreign communication is the broadest of all, it can potentially cover things like email servers, routers, and even personal computers if it can be convincingly proven that they are used in interstate communication. The primary purpose of Section 1030(a)(2) is to protect the confidentiality of computer data, as was noted in 1986 by the Senate Judiciary Committee, they consider that even merely viewing data that is protected by the Section 1030(a)(2) equates to obtaining it.[10]

Section 1030(a)(3) covers unauthorized access to any federal government computer, making it illegal to access any government computer without authorization. While this section seemingly overlaps with section 1030(a)(2), the reasoning behind the two sections is different, section 1030(a)(2) covers the access of federal government computers with the intent of obtaining protected information. Section 1030(a)(3) covers all unauthorized access to federal computers regardless if any information was obtained or not.

Section 1030(a)(4) covers computer fraud and any use of a computer to commit a fraud or to further it falls under this section. But it makes one important exception, it specifically exempts frauds where the only thing of value that was obtained was the use of the computer itself and where the value of such use is not more then $5000 in any one year period. Originally, CFAA did not consider trespass a crime, but Congress recognized that computer use has value of its own but nonetheless included the $5000 threshold to prevent turning every case of trespass into a fraud felony.

Section 1030(a)(5) is perhaps the most widely used section of CFAA, for it covers hacking and malicious code such as viruses and worms that do or attempt to cause damage to protected computers. In essence, it is a crime to cause damage or attempt to cause damage to a computer which would result in financial losses of more then $5000, loss or alteration of medical data, physical injury to a person, a threat to public health safety, or affect administration of justice, national defense, or national security.

[10] Senate Judiciary Committee Report No. 99–432, p. 6–7 (1986)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Section 1030(a)(6) is very simple, it covers trafficking in passwords or similar information which can be used to access computers. This section makes it a crime if such trafficking affects interstate or foreign commerce or the computer in question is in use by the U.S. government.

Section 1030(a)(7) makes it illegal to use interstate or foreign communication to threaten a protected computer with the intent of extorting money or other things of value. The reason this section got implemented was the growing rise of threats directed against computer networks. Section 1030(a)(7) covers the use of any interstate or international communication method when used in transmitting of threats against computers, computer networks, their data and programs, this includes mail, telephone, or any computer communication.

Electronic Communications Privacy Act

Passed in 1986, Electronic Communications Privacy Act (ECPA) was an amendment to the federal wiretap law, the Act made it illegal to intercept stored or transmitted electronic communication without authorization.[11] ECPA set out the provisions for access, use, disclosure, interception and privacy protections of electronic communications. Which is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce." The Act prohibits illegal access and certain disclosures of communication contents. In addition, ECPA prevents government entities from requiring disclosure of electronic communications by a provider such as an ISP without first going through a proper legal procedure.

ECPA was amended in 1994 by the Communications Assistance for Law Enforcement Act (CALEA).[12] CALEA requires the ISPs to build in capabilities into their networks that would allow the law enforcement to carry out electronic surveillance of specific individuals. CALEA did not remove the need for a warrant before such surveillance could be carried out, it only made sure that if there was a need the law enforcement would be able to do so.

Cyber Security Enhancement Act

Cyber Security Enhancement Act (CSEA) was passed together with the Homeland Security Act in 2002, it granted sweeping powers to the law enforcement organizations and increased penalties that were set out in the Computer Fraud and Abuse Act.[13]

---

[11] Electronic Communications Privacy Act, internet, http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act.txt
[12] Communications Assistance for Law Enforcement Act, internet, http://www.techlawjournal.com/agencies/calea/47usc1001.htm
[13] Cyber Security Enhancement Act, internet,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Prior to the passage of CSEA, ISPs were forbidden by the ECPA from knowingly divulging personal details of their customers, for example to gain the contents of an email stored on ISP's servers the government needed a search warrant. CSEA reduced the amount of privacy of stored data, it allows an ISP to voluntarily hand over personal information about its customers to a government agent, not just law enforcement officials, if the ISP has a reason to believe that the information concerns a serious crime. Thus allowing law enforcement to gain access to data without a warrant that they would have previously required. CSEA also allows the ISPs to let the law enforcement to intercept electronic communications on its computers if the ISP believes that they belong to a trespasser who is not authorized by the ISP to be on their computer. Thus completely bypassing any need for a warrant as was previously required.

The Act also authorizes harsher sentences for individuals who knowingly or recklessly commit a computer crime that results in death or serious bodily injury. The sentences can range from 20 years to life. In addition CSEA increases penalties for first time interceptors of cellular phone traffic, thus removing a safety measure enjoyed by radio enthusiasts.

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) was enacted in 1998. The basic purpose of the DMCA is to amend Title 17 of the United States Code and to implement the World Intellectual Property Organization (WIPO) Copyright Treaty and Performances and Phonograms Treaty, which were designed to update world copyright laws to deal with the new technology.[14]

The DMCA prohibits "circumventing a technological measure" designed to protect a copyright. By technological measure DMCA means an access control technology which can take many forms, such as copy protection on CDs, requiring cd-keys or product codes in order to use installed software and so on. As such anyone attempting to disable or bypass such a technological measure would be in violation of the law. DMCA also prohibits the manufacture or sale of devices or programs whose primary purpose is to circumvent access control technology. In addition DMCA prohibits the removal or alteration of information identifying the author, copyright holder, performer, or director of a work, and terms and conditions for use of a work for the purpose of facilitating copyright infringement. The Act provides civil remedies as well as criminal penalties for violating the copyright protection.

DMCA grants several exceptions from its prohibition on circumventing access control measures. It allows reverse engineering for the purpose of achieving interoperability among computer programs, but this only comes into effect if there

---

http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm

[14] The Digital Millennium Copyright Act, internet, http://www.copyright.gov/legislation/dmca.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

is no other way to achieve interoperability and if it is otherwise allowed, and most software licenses usually forbid it. Legitimate research regarding encryption is also exempt from the prohibition as long as the copyrighted work is lawfully obtained, a good faith effort was made to get the owner's permission to break the access control measure, it is necessary for research that is being done and is not forbidden by any other law. The Act of course provides an exemption for the law enforcement and government agencies. The Act also provides an exemption in cases where the security measures are being legitimately checked. In addition DMCA specifically permits the manufacture and sale of technology whose sole purpose is to help parents to control what their children view on the Internet.

The Act includes provisions that provide broad immunity from liability for the ISPs. There is no liability for the ISPs if infringing material is transmitted through their network and computers, so long as the ISP has no control over the content of the materials on its network, and no copy is maintained on the service provider's system. In addition ISPs can not be held liable for infringement for copies of material automatically made for the purpose of temporary storage, i.e., caching. ISPs are also made immune from liability if the infringing materials are stored on their systems, or for links to infringing materials if the ISP has no actual knowledge of the infringing activity, does not receive a financial benefit that can be attributed to the infringing activity in cases where ISP has the right and the ability to control such an activity, and acts expeditiously to disable or remove any infringing material when notified in writing of such an activity.

Other Laws Used to Prosecute Computer Crimes

In addition to laws specifically tailored to deal with computer crimes, traditional laws can also be used to prosecute crimes involving computers. For example the Economic Espionage Act (EEA) was passed in 1996 and was created in order to put a stop to trade secret misappropriation. [15] EEA makes it a crime to knowingly commit an offense that benefits a foreign government or a foreign agent. The Act also contains provisions that make it a crime to knowingly steal trade secrets or attempt to do so with the intent of benefiting someone other then the owner of the trade secrets. EEA defines stealing of trade secrets as copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying trade secrets without authorization. The Act, while not specifically targeted at computer crimes, nonetheless covers the use of computers.

Other federal criminal statutes that are used to prosecute computer crimes are the criminal copyright infringement statute[16], National Stolen Property Act[17] and

[15] Economic Espionage Act of 1996, internet, http://www.ncix.gov/pubs/online/eea_96.htm
[16] 17 U.S.C. §506(a)(1), internet, http://www4.law.cornell.edu/uscode/17/506.html
[17] National Stolen Property Act, internet, http://exchanges.state.gov/culprop/18-2314.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

as I already mentioned the wire fraud statute. In addition to the federal government, many states have also passed computer crime laws. For example in 1999, Virginia passed the Virginia Internet Policy Act, composed of seven bills: Virginia Computer Crimes Act; Encryption Used in Criminal Activity; Encryption Technology; Virginia Computer Crimes Act, Penalties; Freedom of Information; Privacy Protection; and Child Pornography and Indecent Liberties with Children.[18]

Proposed Computer Crime Legislation

The two most significant proposed legislations in the U.S. Congress at this time are the Fraudulent Online Identity Sanctions Act (FOISA)[19] and Computer Software Privacy and Control Act (CSPCA).[20] FOISA attempts to tackle the problem of criminals registering online domains under false identification, it includes a provision that would increase jail times for people who provide false contact information to a domain name registrar and then use that domain to commit copyright and trademark infringement crimes. The law, if passed, would not make providing false contact information to domain name registrars a crime by itself, only if that domain is then used in committing a crime would FOISA be used against the criminal.

CSPCA is meant to deal with the problem of spyware and adware that has plagued so many people. The Act, if passed, would prohibit transmission of software that collects and transmits personal information about the owner or operator of the computer, monitors and transmits web pages accessed by the owner or the operator, or modifies default computer settings such as home page, unless the owner or the operator give their consent and the software has an uninstall option built into it.

Conclusion

While there is no silver bullet for dealing with cyber crime, it doesn't mean that we are completely helpless against it. The legal system is becoming more tech savvy and many law enforcement departments now have cyber crime units created specifically to deal with computer related crimes, and of course we now have laws that are specifically designed for computer related crime. While the existing laws are not perfect, and no law is, they are nonetheless a step in the right direction toward making the Internet a safer place for business, research and just casual use. As our reliance on computers and the Internet continues to grow, the importance of the laws that protect us from the cyber-criminals will continue to grow as well.

---

[18] The Virginia Internet Policy Act, internet, http://www.llrx.com/congress/061599.htm
[19] Fraudulent Online Identity Sanctions Act, internet, http://www.theorator.com/bills108/hr3754.html
[20] Computer Software Privacy and Control Act, internet, http://www.house.gov/inslee/images/spyware.PDF

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

"2003 CSI/FBI Computer Crime and Security Survey".
http://www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm

Atomic Energy Act of 1954,
http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf#pagemode=bookmarks&page=14

Baker, Glenn D. "Trespassers Will be Prosecuted: Computer Crime in the 1990's." Computer/Law Journal Vol. 12, No. 1 (Oct. 1993): 68.

Communications Assistance for Law Enforcement Act,
http://www.techlawjournal.com/agencies/calea/47usc1001.htm

Computer Fraud and Abuse Act of 1986,
http://bar.austlii.edu.au/au/other/crime/123.html

Computer Software Privacy and Control Act,
http://www.house.gov/inslee/images/spyware.PDF

Cyber Security Enhancement Act,
http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm

Digital Millennium Copyright Act,
http://www.copyright.gov/legislation/dmca.pdf

Economic Espionage Act of 1996,
http://www.ncix.gov/pubs/online/eea_96.htm

Electronic Communications Privacy Act,
http://www.cpsr.org/cpsr/privacy/communications/wiretap/electronic_commun_privacy_act.txt

Fraudulent Online Identity Sanctions Act,
http://www.theorator.com/bills108/hr3754.html

National Information Infrastructure Protection Act of 1996,
http://www.epic.org/security/1996_computer_law.html

National Stolen Property Act,
http://exchanges.state.gov/culprop/18-2314.html

Senate Judiciary Committee Report. No. 99–432 (1986): 6–7.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

United States Criminal Code, Title 17 Section 506(a)(1),
http://www4.law.cornell.edu/uscode/17/506.html

United States Criminal Code, Title 18 Section 1030,
http://www4.law.cornell.edu/uscode/18/1030.html

United States Criminal Code, Title 18 Section 1343,
http://www4.law.cornell.edu/uscode/18/1343.html

United States v. Thomas,
http://www.law.emory.edu/6circuit/jan96/96a0032p.06.html

Virginia Internet Policy Act,
http://www.llrx.com/congress/061599.htm

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced