# #

**/etc** (general term): The directory on **UNIX** in which most of the configuration information is kept.

**See Also:** UNIX.

**/etc/passwd** (general term): The **UNIX** file that stores all of the account information, including username, **password** (encrypted form), the user identifier, the primary group the user belongs to, some additional information about the account (such as the real human name or other personal parameters), the user's home directory, and the login **shell**. This file is of particular interest to crackers; if they can read files from this directory, they can use the information to attack the machine.

**See Also:** Password; Shell; UNIX.

**/etc/shadow** (general term): **UNIX** was designed on the concept that the encrypted forms of passwords in the **/etc/passwd** file could be read by those having access to this file, which stored the full account information. However, in practice, users tend to use guessable **passwords**, which can be easily cracked.

A program called "crack" was developed that could guess dictionary words (/usr/dict) and then brute-force the system. Using "crack," researchers found that on an average UNIX system, 90% of all passwords could be cracked with just a few days' worth of computing time. To solve this very real problem, a "shadow" password file was developed for UNIX. Thus, the **encrypted** passwords are removed from the /etc/passwd file and placed in a special /etc/shadow file readable only by root.

**See Also:** Encryption or Encipher; /etc/passwd; Password; UNIX.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website: http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

**/etc/syslog.conf** (general term): The **UNIX** system configuration file describing the system events to be logged either to a **logfile** on the same machine or to a loghost over the network. Information from this file is interesting to **crackers**; they find where their actions are stored so that they can forge the logfiles and hide their tracks.

**See Also:** Crackers; Logfile.

**0wn** (general term): A hacker culture term (typically spelled with a zero and not an O) meaning to control completely. For example, a system broken into by a **hacker** or **cracker** is under complete control of the perpetrator.

**See Also:** Crackers; Hacker.

**2600 Hz** (general term): The tone that long-distance companies such as American Telephone and Telegraph used to indicate that the long-distance lines were open. This knowledge was used by early-day phreaker John **Draper** (a.k.a. Cap'n Crunch) and is the lead-in title for *2600: The Hacker Quarterly*, a popular computer underground magazine.

**See Also:** Bernie S. (a.k.a. Edward Cummings); Draper, John; Goldstein, Emmanuel Hacker Icon (a.k.a. Eric Corley).

# A

**AAA** (general term): AAA stands for **A**uthentication, **A**uthorization, and **A**ccounting. The AAA framework defines a set of functionalities to provide access control to network devices, such as routers, from a centralized location in the network.

**See Also:** Access Control; Access Control System.

**Acceptable Internet Use Policy (AUP)** (general term): A written agreement outlining the terms and conditions of Internet usage, including rules of online behavior and access privileges. Because of the possible misuse of school and division-wide **computer network**s and the Internet by students having access privileges, educational institutions are particularly concerned about having a well-developed AUP in place, which is then signed by the students, their parents (if minors are involved), and their teachers.

Businesses have similar concerns and are also committed to developing AUPs for their computer network and Internet users. Generally, AUPs emphasize the maintenance of courtesy, **accountability**, and **risk** management while working online. A well-constructed AUP, therefore, focuses on responsible use of computer networks, the Internet, and the access and transmission of information to others in the virtual community. An AUP in educational institutions also can include a description of suggested strategies for teaching students using the Internet as well as a delineation of appropriate uses of the Internet in the classroom; a breakdown of appropriate network responsibilities for students, teachers, and parents; a well-delineated code of **ethic**s dealing with Internet and computer network usage; a detailing of the fines and penalties that would be imposed if the acceptable Internet use policies were violated; and a statement regarding the importance of complying with relevant **telecom**munication **laws** and regulations.

**See Also:** Accountability; Computer; Copyright Laws; Ethic; Internet; Network; Risk; Telecom; Violation-Handling Policy; White Hat Hacker.

**Further Reading:** Buckley, J.F., and Green, R.M. *2002 State by State Guide to Human Resources Law.* New York, NY: Aspen Publishers, 2002; Virginia Department of Education Department of Technology. *Acceptable Use Policies—A Handbook.* [Online, July 6, 2004.] Virginia Department of Education Department of Technology Website. http://www.pen.k12.va.us/go/VDOE/Technology/AUP/home.shtml.

**Access Control** (general term): A means of controlling access by users to **computer** systems or to data on a computer system. Different types of access exist. For example, "read access" would suggest that the user has authorization only to read the information he or she is accessing, whereas "write access" would suggest that the user has **authorization** to both read and alter accessed data.

Access control is also an important concept within Web and other applications. The segmentation of functionality, and even entire sections of an application, are based on access control.

**See Also:** Authorization; Computer.

**Access Control List (ACL)** (general term): Used to list accounts having access not only to the computer system in general but also to the information resources to which that list pertains. For example, a system **administrator** can configure firewalls to allow access to different parts of the computer **network** for different users. The ACL, therefore, would include the list of **Internet Protocol (IP)** Addresses having authorized access to various **port**s and information systems through the **firewall**.

An additional layer of security, particularly for Web applications, is provided by reverse proxy servers—technical systems through which requests to a Web applications flow before they get to the application servers. These systems also rely heavily on ACLs to control which IP address ranges are allowed to connect to the service.

The term is also used to describe the security policies in a computer file system.

**See Also:** Administrator; Firewall; Internet Protocol (IP); IP Addresses; Network; Port and Port Numbers.

**Access Control Policy** (general term): Typically, system **administrator**s at the top of organizational and governmental agencies ascertain which individuals or systems will be given access to information. The access control policy outlines the controls placed on both physical access to the computer system (that is, having locked access to where the system is stored) and to the software in order to limit access to **computer network**s and data. Access control policies provide details on controlling access to information and systems, with these topics typically covered at some length: the management of a number of key issues, including access control standards, user access, network access controls, **operating system software** controls, **password**s, and higher-**risk** system access; giving access to files and documents and controlling remote user access; monitoring how the system is accessed and used; securing workstations left unattended and securing against unauthorized **physical** access; and restricting access.

**See Also:** Administrator; Computer; Network; Operating System Software; Password; Physical Exposure; Risk; Superuser or Administrative Privileges.

**Further Reading:** RUSecure. RUSecure Information Security Policies. [Online, 2004.] RUSecure Interactive Security Policies Website. http://www.yourwindow.to/security-policies/sosindex.htm.

**Access Control System** (general term): Including both **physica**l and logical safeguards, the access control system evaluates the security levels of both the user and the **computer** system or data on a system attempted to be accessed. The primary function of this control system is to act as a means of preventing access to unauthorized users. Users are assigned clearance levels, which then gives them access to certain types of information on the computer system. Obviously, the users assigned low levels of clearance cannot access confidential or top-secret information.

**See Also:** Computer; Physical Exposure; Superuser or Administrative Privileges.

**Accountability** (general term): The readiness to have one's actions, judgments, and failures to act to be questioned by responsible others; to explain why deviations from the reasonable expectations of responsible others may have occurred; and to respond responsibly when errors in behavior or judgment have been detected. Accountability, a critical component of professionalism, is closely related to the principles of morality, **ethic**s, and legal obligations. In a computer sense, this term associates computer users with their actions while online.

In recent times, accounting corporate scandals at Enron, WorldCom, and Nortel have resulted in corporate leaders' being held accountable for their misdeeds, with some serving time in prison.

Alberta-born, one-time **Telecom** tycoon Bernard Ebbers, for example, was found guilty on March 15, 2005, of conducting the largest accounting fraud in U.S. history. His convictions on all nine counts and on the $11 billion fraud carry a cumulative maximum jail time of 85 years. Ebbers' case is a continuation of white-collar crime exposure that made media headlines at the end of the 1990s when the high-tech bubble burst. The role of executive and board accountability has since become a major business issue in this millennium, with new laws being passed in the United States and elsewhere for dealing with corporate accountability infractions. More recently, on May 25, 2006, the U.S. government Enron task force was praised publicly when guilty verdicts were announced against former chair Kenneth Lay and former CEO Jeffrey Skilling, the two top executives most accountable for the Enron corporation's collapse. Lay, convicted of 6 charges of conspiracy and securities and wire fraud, faces a maximum of 165 years behind bars, while Skilling, convicted of 19 counts of conspiracy, securities fraud, lying to auditors, and insider trading, faces a maximum sentence of 185 years behind bars.

Moreover, with the passage of the Sarbanes-Oxley Act of 2002 (SOX) in the United States, any breach in Information Technology security represents a **risk** to the information stored on company computers and could be viewed as a violation of Section 404 of the Act—a major issue pertaining to accountability. In short, Section 404 requires company corporate leaders and third-party auditors to certify the effectiveness of internal controls put in place to protect the **integrity** of financial reports—processes as well as technologies. In other words, a corporate leader's lack of control over Information Technology (IT) **security** might reasonably imply a lack of control over the organization's financial reports, a violation of section 404 of the Act. The Chief Executive Officer (CEO) or the Chief Information Officer (CIO) could, indeed, be held accountable for a breach of the Act.

As a result of the importance of corporate accountability with regard to SOX compliance, security information management (SIM) solutions are an emerging product group that will enable CEOs and CIOs to comply with the conditions defined in the Sarbanes-Oxley Act by providing rapid threat detection to the system, management of the threat, and containment. Real-time security monitoring and correlation solutions are a key means of having companies comply. Moreover, if challenged in court with violating provisions of the Act, CEOs and CIOs using SIM solutions will be able to provide a reporting and complete logging of incidents to show that security policies not only were in place but also were being followed correctly and in a consistent, compliant, accountable manner.

A typical SIM system collects **logfiles** and incident data from a number of network and server sources; correlates these incidents in real time to identify potential threats before they materialize into real threats; prioritizes threats based on risk weightings, target **vulnerabilities**, and other key variables; maintains a known threats and vulnerability information data set; and allows for automated as well as guided operator system actions to help the company provide for a reliable and consistent set of incident responses.

**See Also:** Ethic, White Hat Hacker; Integrity; Logfiles; Risk; Security; Telecom; Vulnerabilities of Computers.

**Further Reading:** Bednarz, A. Offsite Security Complicates Compliance. [Online, March 22, 2005.]

Network World Inc. Website. http://www.nwfusion.com/news/2005/0318offsite.html; Hollows, P. Hackers Are Real-Time. Are You? [Online, February 28, 2005.] Simplex Knowledge Company Website. http://www.s-ox.com/Feature/detail.cfm?ArticleID=623; Houpt, S. Ebbers' Storied Career Ends With Record-Fraud Conviction. *The Globe and Mail*, March 16, 2005, p. B1, B7; Hunt, G. 1999. Accountability. [Online, 1999.] Freedom to Care Website. http://www.freedomtocare.org/page15.htm.

**Account Harvesting** (general term): Often used to refer to **computer spammers**, individuals who try to sell or seduce others through **email** advertising or solicitation. Account harvesting involves using computer programs to search areas on the Internet in order to gather lists of email addresses from a number of sources, including chat rooms, domain names, instant message users, message boards, news groups, online directories for Web pages, Web pages, and other online destinations. Recent studies have shown that newsgroups and **chat rooms**, in particular, are great resources for harvesting email addresses.

Search engines such as Google have become an excellent source of email addresses. With a simple automated search using the search engine's API (Application Programmers Interface), an individual can get all email addresses that were collected by the search engine. In particular, it is of interest when an account-harvesting effort targets a particular domain, such as launching a **spear phishing** attack against a target.

Preventative measures for harvesting include masking email addresses for harvesting software, using a separate screen name for online chatting that is not associated with one's email address, setting up two separate email addresses—one for personal messages and another for public posting, and using unique email addresses that combine letters and numbers.

**See Also:** Chat Room; Computer; Electronic Mail or Email; Spam; Spammers; Spamming/Scrolling.

**Further Reading:** Federal Trade Commission (FTC). Email Address Harvesting: How Spammers Reap What You Sow. [Online, November, 2002.] Federal Trade Commission Website. http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm; Martorella, C. Google Harvester. [Online, April 5, 2006.] http://www.edge-security.com/soft/googleharvester-0.3.pl.

**Active Attack** (general term): Carries out an action against the targeted **computer** system—such as taking it offline, as in **Denial of Service** (**DoS**). An active attack could also be made to target information by altering it in some way—as in the defacement of a Website. A passive computer attack, in contrast, simply eavesdrops on or monitors targeted information but does not alter it.

**See Also:** Computer; Denial of Service (DoS); Passive Attack.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

**Active Countermeasures** (general term): Active countermeasures fall into two main categories. The first category includes the countermeasures taken by the security analyst as a reaction to an alarm of an **Intrusion Detection System** (**IDS**), or the countermeasures an **Intrusion Prevention** System (IPS) takes to block an **Active Attack** and to prevent the attacker from doing further harm.

The second category is more controversial. Here, the defender attempts to identify the attacker and then tries to stop the attack by actively exploiting vulnerabilities in the attacker's computer. The legality of such an extreme countermeasure is currently being discussed in legal circles, and to date, no cases have been tried to indicate how the courts would rule in these cases.

**See Also:** Active Attack; Intrusion Detection System (IDS); Intrusion Prevention; Passive Countermeasures.

**ActiveX** (general term): A set of technologies developed by Microsoft Corporation that evolved from two other Microsoft technologies: OLE (Object Linking and Embedding) and COM (Component Object Model). ActiveX controls, widely written about, are among the many types of components to provide interoperability with other types of Component Object Model services.

Specifically, ActiveX controls provide a number of enhancements designed to not only aid in the distribution of components over **network**s but also to provide for the integration of controls into Web **browser**s. To control **malicious code** (such as **virus**es and **worm**s), for example, ActiveX relies upon **digital signature**s and zones. That is, Microsoft browsers have been configured to allow ActiveX programs from servers in the trusted zone and to deny unsigned programs from servers in untrusted zones. Though the concept of **trust**ed zones and digital signatures works well in theory, a variety of destructive worms in recent years (such as Melissa) that have worked their way through Microsoft Web browsers have shown that this theory has flaws.

**See Also:** Browser; Code or Source Code; Digital Signature; Malicious Code; Trust; Virus; Worm.

**Further Reading:** Jupitermedia Corporation. Active X. [Online, July 6, 2004.] Jupitermedia Corporation Website. http://www.webopedia.com/TERM/A/ActiveX.html; Microsoft Corporation. ActiveX Controls. [Online, 2002.] Microsoft Corporation Website. http://www.microsoft.com/com/tech/ActiveX.asp.

**Activity Log** (general term): An activity log is a report in which all the recorded computer events are sequentially ordered and displayed.

**Adams, Douglas** (person; 1952–2001): Wrote *The Hitchhiker's Guide to the Galaxy* and became a household word when the cult science fiction novel was converted into a British Broadcasting Corporation television series. Adams also was held in high regard in the **Computer Underground** because his book demonstrated much of the *zen*-like thinking used in hacking. The book sold more than 14 million copies globally. In May 2005, a film of the same title was released by Buena Vista Pictures. Other books by Adams include *The Restaurant at the End of the Universe*; *Life, the Universe and Everything*; and *So Long and Thanks for All the Fish; Mostly Harmless*.

Adams was a very creative individual with a sense of humor. His *Hitchhiker's Guide to the Galaxy* detailed the universal journey of Ford Prefect, an alien, and Arthur Dent, a human, after Earth was destroyed. On a deeper plane, the story focused on the search for an answer to life as well as to the universe. It turns out that the answer was 42.

Terminology introduced in Adams' books found its way into the hacker jargon. For example, the word "bogon" was used falsely by Arthur Dent, one of the main characters in *The Hitchhiker's Guide to the Galaxy*, to describe the Vogons, an alien race. This term has been adopted by the computer underground to describe erratic behavior of **network** equipment, such as "the network is emitting bogons."

The h2g2 Website that Douglas Adams helped design was groundbreaking in the sense that it not only culminated from his childhood dreams but also enabled an online encyclopedia to be created—in his terminology—by the people for the people. Adams was educated at Cambridge University's St John's College. He was also an **Internet** pioneer who believed that something powerful was created when people pooled their experiences and information; he said that this is just what the Internet did, and he presented a series on the marvels of the Internet on BBC radio. He died suddenly at age 49 on May 14, 2001.

**See Also:** Computer Underground (CU); Internet; Network.

**Further Reading:** Buena Vista. The Hitchhiker's Guide to the Galaxy. [Online, May 15, 2005.] Buena Vista Website. http://hitchhikers.movies.go.com/hitchblog/blog.htm; Yentob, A. Author Douglas Adams Dies. [Online, May 14, 2001.] BBC News Website. http://news.bbc.co.uk/1/hi/uk/1326657.stm.

**Address Verification** (general term): A mechanism used to control access to a wired or **wireless computer** network. Before a newly connected computer is allowed to communicate over the network, its hardware address (**MAC Address**) is checked against a list of known and permitted computers. MAC addresses are used to uniquely identify the network card of a computer. Address verification is not a tamper-proof mechanism to prevent connection from unauthorized computers because attackers can "spy out" valid MAC addresses and set their MAC address to spoof an otherwise authorized address, thus gaining access to the **network**.

**See Also:** Computer; Message Authentication Code Address (MAC Address); Network; Wireless.

**ADM (ADMw0rm Internet) Worm of 1998** (general term): A collection of programs written to automatically exploit **vulnerabilities** in **Linux** systems to gain access, attack other systems from compromised hosts, and copy itself to vulnerable systems. This worm was seen in the period May 1, 1998, to late May 1998. When this worm hit, compromised systems were left with a "w0rm" backdoor account. The target's **Internet Protocol** (**IP**) Address was then **email**ed to the worm's developers. All **logfiles** in the targeted directory were deleted, and all index.html files on the file system were located and replaced with the words "The ADM Internet w0rm is here!"

**See Also:** Electronic Mail or Email; Internet Protocol (IP); IP Address; Linux; Logfiles; Malware; Vulnerabilities in Computers; Worm.

**Further Reading:** Nazario, J. Defense and Detection Strategies against Internet Worms. [Online, 2004.] VX Heavens Website. http://vx.netlux.org/lib/anj01.html#c421/.

**Administrator** (general term): A key role played by a computer professional who oversees the **network** operation, installs programs on a network, configures them for distribution, and updates **security** settings. These tasks can be performed on various levels. System administrators look after operating systems, and network administrators take care of the network devices. On the application layer, database administrators maintain database management systems, whereas Webmasters oversee Web applications, servers, and services.

**See Also:** Network; Security; System Administration Theory.

**Advanced Encryption Standard (AES)** (general term): An encryption methodology developed by the United States **National Institute of Standards and Technology (NIST)** and publicized as a Federal Information Processing Standard (FIPS). AES is a privacy transformation for **Internet Protocol Security** (**IPSec**) and Internet **Key** Exchange (IKE). AES was designed not only to replace the **Data Encryption Standard** (**DES**) but also to be more secure than its predecessor. Compared to DES, AES offers a large key size and ensures that the only known approach to **decrypt** messages is for cyber-intruders to try every possible key—a daunting task indeed. The AES has variable key lengths, with algorithms specifying a 128-bit key (the default), a 192-bit key, and a 256-bit key. Although AES was developed to replace DES, NIST suggests that DES will remain an approved **encryption algorithm** for the near future.

**See Also:** Algorithm; Data Encryption Standard (DES); Decryption or Decipher; Encryption or Encipher; Internet Protocol Security (IPSec); Key; National Institute of Standards and Technology (NIST).

**Further Reading:** Cisco Systems, Inc. Advanced Encryption Standard (AES). [Online, March 2, 2004.] Cisco Systems, Inc. Website. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/.

**Advanced Research Projects Agency Network (ARPANET)** (general term): Established in 1969 by the United States Defense Advanced Research Project Agency (DARPA), the ARPANET, a wide-area network (**WAN**), linked universities and research centers—such as the University of California at Los Angeles, the University of Utah, and the Stanford Research Institute (SRI). All of these centers were involved in developing new networking technologies. ARPANET was to research how to utilize DARPA's investment in **computer**s through Command and Control Research (CCR). The first leader of ARPANET, Dr. J.C.R. Licklider, was focused on moving the department's contracts away from independent corporations and pushing them toward the best academic computer centers. Another major function of ARPANET was to act as a redundant **network** capable of surviving a nuclear war.

**See Also:** Computer; Defense Advanced Research Projects Agency (DARPA); Network; Wide Area Network (WAN).

**Further Reading:** Hauben, M. Part I: The history of ARPA leading up to the ARPANET. [Online, December 21, 1994.] Hauben's Columbia University History of ARPANET Website. http://www.dei.isep.ipp.pt/docs/arpa--1.html; Jupitermedia Corporation. ARPANET. [Online, July 2, 2001.] Jupitermedia Corporation Website. http://www.webopedia.com/TERM/A/ARPANET.html.

**Advocacy** (general term): Generally, a type of problem solving designed to protect the personal and legal rights of individuals so that they can live a dignified existence. Many types of advocacy exist, with system advocacy being used to change systems and to promote social causes, and with legislative advocacy being used to change **laws**. Regardless of type, effective advocacy generally involves a broad-based approach to problem solving.

With regard to advocacy and digital world issues, three organizations have become recognized for their efforts in this regard: the **Electronic Frontier Foundation** (**EFF**); the Electronic Privacy Information Center (EPIC); and the **Center for Democracy and Technology** (**CDT**).

The EFF is a modern group of freedom fighters who argue that if the United States' Founding Fathers had anticipated the digital frontier, they would have put a clause in the Constitution for protecting individuals' rights online. Thus, the EFF is a group of lawyers, technologists, volunteers, and visionaries who challenge legislative measures threatening basic human rights with online activities.

EPIC, a public interest research center housed in Washington, D.C., was established in 1994. EPIC's purpose is to focus the public's attention on civil liberties issues in the information age and to protect **privacy**, the First Amendment, and values inherent in the Constitution. EPIC publishes an email and online newsletter on topics related to civil liberties in the information age. EPIC also cites reports and books on privacy, open government, free speech, and other topics on civil liberties issues.

The CDT promotes digital age democratic values and constitutional liberties, and for this reason, its members have expertise in law, technology, and policy.The CDT seeks practical solutions to improve free expression and privacy in worldwide communications technologies. Moreover, the CDT is dedicated to bringing together segments interested in the future of the **Internet**. Recent topics of interest to the CDT include the Child Online Protection Act (COPA), the use of **spyware**, and **Spam**.

**See Also:** Center for Democracy and Technology (CDT); Electronic Frontier Foundation (EFF); Internet; Privacy; Privacy Laws; Spam; Spyware.

**Further Reading:** Electronic Frontier Foundation. About EFF. [Online, August 9, 2004.] Electronic Frontier Foundation Website. http://www.eff.org/about/; Electronic Frontier Foundation. Our Mission: With Digital Rights and Freedom For All. [Online, July 5, 2004.] Electronic Frontier Foundation Website. http://www.eff.org/mission.php; Head Injury Hotline. Advocacy Skills. [Online, 1998.] Seattle, Washington Brain Injury Resource Center Website. http://www.headinjury.com/advocacy.htm.

**Adware** (general term): Software delivering pop-up advertisements based on Websites that online users browse. Online users find adware to be particularly annoying, and computer critics maintain that adware often degrades computer performance. It can also track users' browsing habits and is generally installed without users' permission.

Claria Corporation, previously called Gator Corporation, a pioneer of such software, said in March 2006 that it was leaving this business by June 2006. Claria officials maintain that they have hired Deutsche Bank Securities, Inc., to sell their adware assets. Claria is now interested in focusing on PersonalWeb, a new service generating personalized Web portals. Previously, Claria's software came bundled with free products such as the eWallet password-storage program or file-sharing software such as KaZaA.

**Further Reading:** In Brief. Adware Pioneer to Exit Business. *The Globe and Mail*, March 23, 2006, p. B13.

**AFAIK** (general term): An abbreviation used by computer users to mean "as far as I know."

**AFK** (general term): An abbreviation used by computer users to mean "away from keyboard."

**AfriNIC** (general term): The Regional Registry for Internet Number Resources for Africa. It is based in Mauritius.

**See Also:** APNIC; ARIN; LatNIC; RIPE.

**Further Reading:** AfriNic Website [Online, Apr 10, 2006.] http://www.afrinic.net/.

**Aladdin-Esafe Software** (general term): Developed by Aladdin, a company involved in digital **security** that has been providing software solutions for e-business and **Internet** security since 1985, the Aladdin-Esafe software features high-performance, proactive inspections of digital content to stop **spam**, **viruse**s, and **worm**s in their tracks. Aladdin-Esafe software is a **Linux**-based appliance used by a number of large banks around the globe (including the Bank Hapoalim in Israel) to keep their online services and email clean of malicious code. The Aladdin-Esafe software, an application-filtering technology, addresses the latest generations of cyber threats, including malicious code attacks at the network level, Instant Messaging, and **spyware**. This software has won a number of awards for its innovative contributions to the safety of the cyber world, including ***PC** Magazine*'s Editor's Choice in 2002 and the Best Product of 2002 in the Networking Category.

**See Also:** Internet; Linux; Security; Spam; Spyware; Virus; Worm.

**Further Reading:** Aladdin. Bank Hapoalim Chooses Aladdin eSafe. [Online, April 15, 2004.] Aladdin Website. http://www.ealaddin.com/news/2004/eSafe/Bank_Hapoalim.asp; Ziff Davis Media. Aladdin eSafe Appliance. [Online, January 1, 2003.] PC Magazine Website. http://www.pcmag.com/article2/0,1759,758515,00.asp.

**Algorithm** (general term): A set of rules and procedures for resolving a mathematical and/or logical problem, much as a recipe in a cookbook helps baffled cooks in the kitchen resolve meal problems. A **computer** program can be viewed as an elaborate algorithm, and in computer science, an algorithm usually indicates a mathematical procedure for solving a recurrent problem. The word *algorithm* is believed to stem from the name of a mathematician at the Royal Court in Baghdad, Mohammed ibn-Musa al-Khwarizmi (780–850 a.c.).

Today, information security professionals in particular are concerned with **cryptographic** algorithms—those used to **encrypt,** or encode, messages. Different algorithms have different levels of complexity, which is related to key size. For example, a 41-bit key is twice as hard to crack, or decode, as a 40-bit key. A 128-bit key is a trillion times harder to crack than a 40-bit key.

**See Also:** Computer; Cryptography or "Crypto"; Encryption or Encipher.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham's Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html; TechTarget. SearchVB.com Definitions: Algorithm. [Online, July 6, 2004.] TechTarget Website. http://searchvb.techtarget.com/sDefinition/0,,sid8_gci211545,00.html.

**Al-Qaeda** (general term): An international fundamentalist Islamic organization founded by Osama bin Laden in the 1990s and classified as an international terrorist organization by the United States, the European Union, and various other countries. The September 11, 2001, terrorist attacks are attributed to this organization.

As a result of the capture by the U.S. military of some Al-Qaeda terrorists in recent years, some experts have maintained that Al-Qaeda and other terrorist organizations may start to use computer technology more frequently to commit their acts of **terrorism**. For example, seized computers belonging to al-Qaeda indicate that its members are becoming familiar with cracking tools freely available over the **Internet**. Moreover, as more computer-literate members join the ranks of Al-Qaeda and other terrorist groups, they will bring with them an enhanced awareness of the advantages of a cyber-**attack** against highly networked critical infrastructures. And after a "new information technology" attack gets media attention, it will likely motivate other computer-savvy terrorist groups to use cyber attacks against targeted nations and their people.

Evidence suggests that some of the terrorists in the September 11, 2001, attacks used the Internet to plan their terrorist operations. Mohammed Atta, the so-called spearheader of the attacks, made his airline reservation online, and Al-Qaeda cells reportedly used Internet-based telephony to make contact with other cells overseas. Moreover, in an April 2003 news report on the Public Broadcasting System television news program "Frontline," reporters said that an Al-Qaeda computer seized in Afghanistan had models of dams as well as computer programs to analyze them. And on April 22, 2005, Zacarias Moussaoui, the 36-year-old Morroccan sometimes called the twentieth hijacker, not only pleaded guilty to charges related to the September 11 air attacks but also announced in court that his primary objective was to crash a Boeing 747 jet into the White House. He said that he was computer savvy and that though he took flight lessons in Oklahoma and Minnesota, he learned most of his flight lessons through a Boeing 747 computer simulator.

The implications of this kind of evidence, terrorist experts maintain, is that al-Qaeda may be using advanced information technology to assist them in future terrorist attacks against targeted nations and may even be employing some highly skilled **crackers** to assist them in their terrorist plans.

**See Also:** Al-Qaeda; Attack; Crackers; September 11, 2001, Terrorist Events; Terrorist-Hacker Links; Terrorism.

**Further Reading:** Freeman, A. Moussaoui Pleads Guilty to Terror Charges. *The Globe and Mail*, April 23, 2005, p. A15; Wilson, C. CRS Report for Congress: Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. [Online, October 17, 2003.] CRS Website. http://www.fas.org/irp/crs/RL32114.pdf.

**Amenaza's SecurITree Software** (general term): Allows system analysts to design system **security** solutions, much as software programs such as CAD (computer-aided drafting and design) allow engineers to design safe bridges or buildings. SecurITree software allows a security expert to mathematically model possible **attack**s against a computer system. The model is known as "an attack tree."

Using a process known as pruning, a security expert can use the capabilities of system attackers and compare them with the resources required to conduct specific attacks—all built into the software model. Attacks considered to be beyond the cracker's capability are then systematically removed from the model. Thus, what remains in the model are the attacks considered to be highly likely and feasible.

This software is a Java-based application that spotlights which of the deficiencies in a computer system most crackers would find enticing, thus allowing a security expert to objectively consider security trade-offs and to set priorities for **risk**-mitigating actions. The SecurITree software creates a model that outlines the various ways that a computer system can be attacked, predicts how potential system intruders will attack by comparing their capabilities with the system's **vulnerabilities**, evaluates the impact of each attack scenario on the system in question, determines the degree of risk affiliated with each attack scenario, and monitors the computer system for signs of attack.

**See Also:** Attack; Risk; Security; Vulnerabilities of Computers.

**Further Reading:** Amenaza Technologies Limited. Attack Tree Methodology. [Online, July 6, 2004.] Amenaza Technologies Limited Website. http://www.amenaza.com/methodology.html; Amenaza Technologies Limited. Product Overview. [Online, July 6, 2004.] Amenaza Technologies Limited Website. http://www.amenaza.com/products.html.

**American National Standards Institute (ANSI)** (general term): Founded on October 19, 1918, the American National Standards Institute (ANSI) is a private, nonprofit organization that has the dual function of both administering and coordinating the U.S. standardization and conformity assessment system. With headquarters in Washington, D.C., the Institute's mission is to improve not only the global competitiveness of U.S. businesses but also the quality of life for U.S. citizens by doing three things: (1) promoting and facilitating voluntary consensus standards; (2) providing conformity assessment systems; and (3) safeguarding their **integrity**.

Though the Institute was started by five engineering societies and three government agencies, it now represents the interests of almost 1,000 companies, organizations, government agencies, and international members. Accreditation by ANSI indicates an acceptance that the procedures used by the standards body meet the multiple and essential requirements of balance, consensus, due process, and openness. To maintain accreditation by ANSI, developers must consistently adhere to the ANSI Essential Requirements governing the consensus development process.

The United States has ANSI as its representative to the International Accreditation Forum (IAF), the International Electrotechnical Commission (IEC), and the International Organization for Standardization (ISO).

ANSI has standardized the C **programming language** and the encoding of characters into a binary format. The C programming language is widely used in the **hacker** community to write programs, and encoding is used to protect data from crackers.

**See Also:** Hacker; Integrity; Programming Languages C, C++, Perl, and Java.

**Further Reading:** American National Standards Institute. About ANSI Overview. [Online, July 6, 2004.] American National Standards Institute Website. http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1.

**American Registry for Internet Numbers (ARIN)** (general term): A nonprofit organization established to administer and register **Internet Protocol** (**IP**) numbers for North America and parts of the Caribbean. ARIN is but one of the five Regional Internet Registries collectively providing IP registrations services globally. ARIN, it should be noted, is not an **Internet Service Provider** (**ISP**).

The mission statement of ARIN includes applying the principles of stewardship, allocating Internet Protocol resources, developing consensus-based policies, and facilitating the healthy advancement of the Internet through positive information and education.

ARIN started administering **IP network**s (routes) in 1997. Networks allocated before 1997 were recorded in the ARIN whois database. ARIN allows the owners of those networks to maintain them free of charge. Networks allocated after 1997 are also recorded in the ARIN whois database, but the owners of those networks are charged a yearly maintenance fee by ARIN. Also, when ARIN allocates a new network, the owner of the new network is charged an annual fee. When an existing network is transferred to a new owner, the new owner is charged the yearly fee whether or not the previous owner was charged a fee.

**See Also:** AfriNIC; APNIC; Internet Protocol (IP); Internet Service Provider (ISP); LACNIC; Network; RIPE NCC.

**Further Reading:** American Registry for Internet Numbers. About ARIN. [Online, 2004.] American Registry for Internet Numbers Website. http://www.arin.net/about_us/index.html. Siemsen, P. Procedures for Routing Registries and the ARIN Whois database. [Online, August 27, 2002.] UCAR Website. http://www.scd.ucar.edu/nets/docs/procs/routing-registries/#intro.

**Amplifier** (general term): An amplifier is a type of system on the **network** used to increase the size of traffic directed at a specific target. For example, if a **cracker** uses a **smurf** amplifier to attack a target, he or she spoofs the address of the target and sends directed broadcasts to the smurf amplifier, which then sends hundreds or more replies to the target at the mere cost of a single **packet**.

**See Also:** Cracker; Network; Packet.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

***Anarchist Cookbook*** (general term): Written during the late 1960s by William Powell, it delivered the message that violence is an acceptable means to effect political change. The information in the book, which was released in 1970 by Lyle Stuart, Inc., Publishers, contained bomb and drug recipes copied from military documents stored in the New York City Public Library.

Now, Powell maintains that the book was a misguided product of his young adulthood anger, triggered by the possibility that he would be drafted and sent to fight in the Vietnam war—a war that he says he did not believe in. Powell admits to no longer believing in the book's philosophy, and in 1976 when he became a confirmed Anglican Christian, he asked the publisher to stop publishing the book. However, insisting that the **copyright** was in the publisher's name, the publisher did not grant Powell's request.

In the early 1980s, the book rights were sold to another publisher, who, against Powell's wishes, published the book with the original bomb and drug recipe content. Powell receives no royalties from the sale of the book, currently published by Ozark, and a number of **Internet** Websites continue to market the book.

The original version of the book spawned a series of documents that described techniques for cracking computer systems, thus providing a source of education for the neophyte members in the **Computer Underground**.

**See Also:** Computer Underground (CU); Copyright; Copyright Laws; Internet.

**Further Reading:** Powell, W. *The Anarchist Cookbook* by William Powell: Editorial Reviews From the Author. [Online, July 6, 2004.] Amazon Website. http://www.amazon.com.

**Anonymous** (general term): **Computer crackers** commonly attempt to exploit a computer system by sending messages in an anonymous fashion—protecting their identity from being disclosed. Anonymous accounts are used widely to access information and software-sharing systems on computers mainly using the **FTP**. The user accesses the systems by utilizing a user name of "anonymous" or "guest" without a password.

**See Also:** Computer; Crackers; File Transfer Protocol (FTP).

**Anonymous Digital Cash** (general term): Systems allowing individuals to anonymously pay for goods or services by transmitting a cash number from one computer to another are permitting business exchanges through the use of anonymous digital cash certificates. One feature of digital cash certificates is that, as with tangible dollar bills, they are anonymous and reusable. Although credit cards can be traced to a single owner, as with real money digital cash certificates of varying denominations can be recycled. When an individual purchases digital cash certificates, money is withdrawn from a bank account. The certificate is then transferred to a vendor to pay for a product or service. The vendor can then deposit the cash number in any bank or retransmit it to another vendor, and the cycle of transmission can continue.

Combined with **encryption** and/or **anonymous remailers**, digital cash allows **cybercriminals** to make transactions with complete anonymity. This is a common means of not only trafficking in stolen intellectual property obtained on the Web but also extorting money from targets.

In May 1993, for example, Timothy May wrote a piece about an organization called BlackNet that would hypothetically engage in commerce using a combination of anonymous digital cash, anonymous remailers, and public key cryptography. Although May said that he wrote the piece to disclose the difficulty of "bottling up" new technologies, rumors on the **Internet** spread that actual BlackNets were being used by criminals for selling stolen trade secrets.

**See Also:** Anonymous; Anonymous Remailers; Cybercrime and Cybercriminals; Encryption or Encipher; Internet.

**Further Reading:** Jupitermedia Corporation. Digital Cash. [Online, September 1, 1996.] Jupitermedia Corporation Website. http://www.webopedia.com/TERM/D/digital_cash.html; May, T.C. BlackNet Worries. In P. Ludlow (ed.), *High Noon on the Electronic Frontier.* Boston: MIT Press, 1996.

**Anonymous or Masked IP Address** (general term): A means by which crackers can visit **Internet Protocol (IP)** Websites without leaving a trace of their visit. Every computer connected to the Internet has a unique IP address (just as every house on a street has a unique street address). If the IP address is always the same when any given computer connects to the network, it is referred to as a static address. However, when a random IP address is assigned every time a computer connects to the network, it is referred to as a dynamic IP address.

**Crackers** have a number of means of accessing services and computers on the Internet without leaving a trace. One of the most popular tools is called "The Anonymizer," which allows for **anonymous** surfing using either a free service or a fee-for-service. The shortcoming of this tool is that a few Websites are inaccessible, particularly Web-based free email services. Another tool used by crackers located in Germany, in particular, is called Janus. An alternative to The Anonymizer, Janus is free and fast and can encrypt the **URL** and pass it to the server without allowing the user to receive information about the server address. Also, crackers can mask their Web surfing by using a proxy server; Web pages are retrieved by the latter rather than by the cracker browsing the Web. The shortcoming associated with proxy **server**s is that they slow down the data transfer rate and place additional loads on the network and the servers.

A list of available proxy servers can be found at http://tools.rosinstrument.com/cgi-bin/dored/cgi-bin/fp.pl/showlog. However, these lists frequently contain inactive servers or nonworking servers. To avoid wasting the effort of contacting inactive servers, an individual can use tools such as proxyfinder, which can be used to detect live and active proxy servers.

It should be noted that using proxy servers for purchasing items with a bogus credit card number is illegal and, if detected by legal authorities, can lead to imprisonment. Because all connections are logged, a Website **administrator** can review the logs, communicate with the proxy's administrator, and discover the perpetrator's real IP address. Together, they can contact the perpetrator's **Internet** Service Provider, which also keeps **log**s. This is the manner in which system administrators assist law enforcement in capturing crackers intent on committing a crime through computers using anonymous IP addresses.

**See Also:** Administrator; Anonymous; Cracker; Internet; Internet Protocol (IP); IP Address; Log, Server; URL or Uniform Resource Locator.

**Further Reading:** Link Exchange. Hiding Your IP Address or Anonymous Internet Surfing HOWTO. [Online, July 6, 2004.] Link Exchange Website. http://tools.rosinstrument.com/proxy/howto.htm; Proxy Finder Website. [Online, April 5, 2006.] http://www.edge-security.com/soft/proxyfinder-0.3.pl.

**Anonymous Remailers** (general term): **Anonymous** remailers send electronic messages without the receiver's knowing the sender's identity. For example, if a **cybercriminal** wanted to send an anonymous message to a target, instead of emailing the target directly, the initiator could send the message to a remailer (an **email server**), which strips off the identifying headers and forwards the contents to the target. When the target receives the message from the perpetrator, though he or she can see that it came via a remailer, he or she cannot determine the actual sender. During his term in office, President Bill Clinton reportedly received email death threats routed through anonymous remailers.

**See Also:** Anonymous; Cybercrime and Cybercriminals; Electronic or Email; Server.

**Further Reading:** Schell, B.H., Dodge, J.L., with S.S. Moutsatsos. *The Hacking of America: Who's Doing It, Why, and How.* Westport, CT: Quorum Books, 2002.

**Anti-Virus Emergency Response Team (a.k.a. AVERT)** (general term): Headquartered in Santa Clara, California, the **McAfee**, Inc. Anti-Virus Emergency Response Team (known as AVERT) sets out to provide enterprises, government agencies, and institutions with essential services needed to respond rapidly to **intrusion**s on desktop **computer**s, **server**s, and the **network**. AVERT also strives to protect systems from the next version of blended attacks by worms and viruses. AVERT not only keeps track of the most recent viruses and **Trojan** horses to help system administrators become aware of the many new and altered **virus**es emerging daily but also offers solutions for dealing with the cyber problem.

The name of recognized viruses and worms, their date of discovery, as well as the risk to home computers and corporate computers are detailed on http://vil.nai.com/VIL/newly-discovered-viruses.asp.

**See Also:** Computer, Intrusion; Network; Malware; Server; Trojan; Virus; Worm.

**Further Reading:** Networks Associates Technology. McAfee: About Us. [Online, July 6, 2004.] McAfee Security Website. http://www.mcafeesecurity.com/us/about/home.htm?wt.mc_n=ys-about&wt.mc_t=ext_lic.

**Anti-Virus Software** (general term): Detects **virus**es and notifies the user that a virus is present on his or her **computer**. This kind of software keeps a data set of "fingerprints" on file—characteristic bytes from known viruses. The anti-virus software then searches files and programs on a computer for that fingerprint, and when it discovers a recognized fingerprint belonging to a virus, the anti-virus software alerts the user.

Virus writers have begun to use **code**-morphing techniques to avoid detection by anti-virus software by altering the machine code of the virus program while maintaining its malicious functionality. Thus, the signature of the virus is changed and detection by anti-virus software is avoided.

In short, anti-virus software is not foolproof. On February 25, 2005, for example, a critical vulnerability was reported in the anti-virus engine used by Trend Micro's complete product line of client, server, and gateway security products. For that month alone, it was, in fact, the third report of flaws found in recognized security firms' anti-virus software.

Although reported vulnerabilities in security products are more rare than they are in operating systems such as Windows, they do indeed exist. For example, the well-recognized Symantec company has had 108 reported **vulnerabilities** in its products (including Anti-Virus, Norton Utilities, Raptor Firewall, NetProwler, Anti-Spam, Web Security, Gateway, and others). Trend Micro has had 59 reported vulnerabilities in its products (including OfficeScan and VirusBuster), and F-Secure has had 12 reported vulnerabilities in its products (including Policy Manager, Backweb, and Anti-Virus).

Therefore, because anti-virus software products do have vulnerabilities, they tend to provide a false sense of security to purchasers who think they are 100% reliable. Though users buy **firewall**s to halt "bad traffic," they can inadvertently install software that allows intruders into their system.

**See Also:** Code or Source Code; Computer; Firewall; Virus; Vulnerabilities in Computers.

**Further Reading:** Keizer, G. Security Firms Follow Unwritten Code When Digging Up Dirt on Each Other. [Online, February 25, 2005.] CMP Media LLC Website. http://www.informationweek.com/story/showArticle.jhtml;jsessiionid=POBBDHOZK2B4AQSNDBCCKHOCJUMEKJVN?articleID=60403683; Schell, B.H. and Martin, C. *Contemporary World Issues Series: Cybercrime: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, 2004.

**Antonelli, Kay McNulty Mauchly** (person; 1921–2006): Kay McNulty graduated from college in 1942 as one of fewer than a handful of mathematics majors in a class of 92 women. During the summer of Kay's graduation, the U.S. army was recruiting women with degrees in mathematics to calculate by hand the firing trajectories of artillery used for the war.

Kay joined as a "human computer," and while working at the Moore School of Engineering at the University of Pennsylvania, Kay met John Mauchly, a physics professor at Ursinus College. His famous exploit was the co-invention with Presper Eckert of the first electronic computer in 1935, known as the ENIAC (Electrical Numerical Integrator and Calculator).

In 1948, Kay and John wed, and two years later, the couple joined forces with Presper Eckert to start a small computer company. The team of three worked on the development of the Univac (Universal automatic **computer**), known for its expediency. This computer's primary asset was that it used magnetic tape storage to replace bulky punched data cards and printers. On a side note, by 1950 the computer industry was only four years old.

**See Also:** Computer; Mauchly, John.

**Further Reading:** Schell, B.H., Dodge, J.L., with S.S. Moutsatsos. *The Hacking of America: Who's Doing It, Why, and How.* Westport, CT: Quorum Books, 2002.

**AOL Inc. (America Online.com)** (general term): A popular **Internet Service Provider** (**ISP**), provides an **Internet** connection to subscribers—whether they are on a high-speed or dial-up connection—and delivers to subscribers communication tools that are innovative and relatively secure.

In 2005, AOL's users of the instant messaging service could see—using their Microsoft Outlook email application—whether their friends were online. Essentially, the AOL tool goes through users' Outlook address books and matches email addresses with the corresponding AIM screen anems that AOL collected during the registration process. With this communication tool, users could manually add screen names. Though initially users needed the latest version of AIM software available as a "beta" test download for Windows computers, currently users are able to send and receive messages from any Web browser. Each account has two gigabytes of storage—about the same storage as Google Inc.'s Gmail and greater than that offered by Yahoo! Inc. and Microsoft Corporation.

AOL, Inc. has not been free of **cybercrime** issues. On January 23, 2003, for example, Brian T. Ferguson was found guilty of **cracking** the AOL account three times of Judge Kim D. Eaton, who handled the 43-year-old's divorce case. Through this crack exploit, Ferguson obtained personal email messages of Judge Eaton, as well as computer files and other data that were part of her AOL account. To prove that he had access to her AOL account, Ferguson appeared before Judge Eaton in April 2002, handing her some email messages that she had sent to various people. Especially upsetting to the judge was the fact that the emails had personal information about her children's activities. The judge further noted in a court hearing regarding this cybercrime that Ferguson's remarks led her to believe that he was a threat to her and her close family members. Because of this cybercrime, Ferguson faced a possible prison sentence of three years and a fine of $300,000.

**See Also:** Cracking; Cybercrime and Cybercriminals; Internet; Internet Service Provider (ISP).

**Further Reading:** America Online. What is AOL? [Online, July 6, 2004.] America Online Website. http://www.AOL.com; In Brief. AOL Offers Free E-mail Tied to Its Instant Messaging. *The Globe and Mail*, May 12, 2005, p. B8; In Brief. AOL Ties Buddy Lists to Microsoft Outlook. *The Globe and Mail*, March 3, 2005, p. B10; Schell, B.H. and Martin, C. *Contemporary World Issues Series: Cybercrime*: *A Reference Handbook*. Santa Barbara, CA:ABC-CLIO, 2004.

**Apache Software Foundation (ASF)** (general term): A nonprofit corporation that evolved from the Apache group who convened in 1995 to develop the now-popular Apache **HTTP server** (which runs on such **operating system software** as **Linux**, **Solaris,** and Windows). Some experts maintain that Apache is the most widely used Web server software.

Currently, the Apache Software Foundation gives support to Apache open-source software projects—characterized by a process that is collaborative, involves a consensus, and strives to produce leading-edge, high-quality software. A stated purpose of foundation members is to produce open and practical software licenses. The Foundation was formed for a number of reasons, including to provide a communication forum and a business infrastructure to support open, collaborative software development projects.

The Foundation's functions also included the creation of an independent legal group to which individuals and firms could donate resources and be assured that the resources would be used strictly for the public benefit. The independent legal group was also to provide a means for volunteers to be protected from lawsuits aimed at the Foundation's projects and to protect the "Apache" brand (as applied to software products) from being abused by organizations.

Membership in the Apache Software Foundation is based on merit and requires that one be an active project contributor. New candidates are nominated by an existing member, and a vote of all members is then taken. The candidate must win a majority vote to be given full membership privileges. The current list of ASF members is detailed at http://www.apache.org/foundation/members.html.

**See Also:** HTTP (HyperText Transfer Protocol); Linux; Operating System Software; Server; Solaris.

**Further Reading:** The Apache Software Foundation. Frequently Asked Questions. [Online, July 6, 2004.] The Apache Software Foundation Website. http://www.apache.org/foundation/faq.html.

**Application Floods** (general term): See **Denial of Service** (**DoS**).

**Archie** (general term): A system for locating files stored on **FTP server**s.

**See Also:** File Transfer Protocol (FTP); Server.

**Area Code Fraud** (general term): Because some countries in the Caribbean have what appear to be North American telephone area codes (with the Bahamas having an area code of 242 and the Cayman Islands having an area code of 345), a rather common telephone area code fraud is to fool people into calling these numbers even though they believe that they are telephoning a United States or a Canadian **jurisdiction** where **fraud** laws apply. The unsuspecting target often faces not only large telephone bills but also invoices for products or services that are fraudulent.

A Website with more information on the North American Numbering Plan Administration (NANPA) can be found at http://www.nanpa.com/. This site provides information about the numbering plan for the Public Switched Telephone **Network** for Canada, the United States (and its territories), and the Caribbean.

**See Also:** Fraud; Jurisdiction; Network.

**Further Reading:** NeuStar, Inc. NANPA: North American Numbering Plan Administration. [Online, 2003.] NeuStar, Inc. Website. http://www.nanpa.com/.

**ARIN** (general term): See **American Registry for Internet Numbers**.

**Armouring (virus)** (general term): Using this technique, viruses can stop security analysts from examining their code. That said, if analysts want to learn more about viruses, they must look into files using debuggers—programs allowing them to investigate each line of the virus code in the original language in which it was written. When armouring is present, reading the code becomes impossible. Although viruses utilizing this technique can be detected and then isolated, they make it difficult for analysts to study their functioning as well as detect the routines allowing the antivirus software to "disinfect" it.

**See Also:** Virus.

**Further Reading:** Panda Software. Glossary of Terms. [Online, April 9, 2006.] http://www.pandasoftware.com/virus_info/encyclopedia/glosary.htm#ARMOURING.

**ARP (Address Resolution Protocol)** (general term): A technical term, ARP is a protocol that is used with **TCP/IP** to resolve addresses on the Link Layer of the **Protocol** Stack.

The address resolution protocol (see Figure 1-1) is used to find a hardware address for a given **IP address**. Computer names on the **Internet** are associated with IP addresses. To send a message to a computer via the local network (for example, through **Ethernet** or a wireless network), the hardware address must be known.

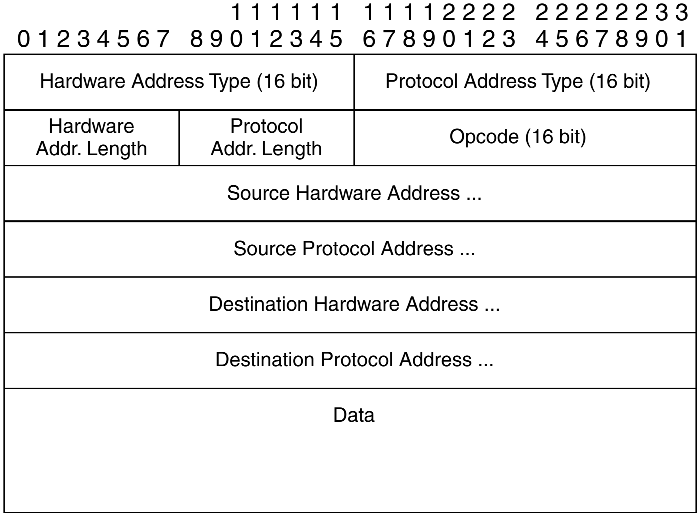
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Hardware Address Type (16 bit)
Protocol Address Type (16 bit)
Hardware Addr. Length
Protocol Addr. Length
Opcode (16 bit)
Source Hardware Address ...
Source Protocol Address ...
Destination Hardware Address ...
Destination Protocol Address ...
Data

**Figure 1-1. The Address Resolution Protocol**

So, when a computer needs to transmit an IP **packet** to a computer in the same network segment, it broadcasts the destination IP address on the local Ethernet using the ARP protocol, where it is read by all attached computers. To achieve this, it fills out the fields of the protocol with its Ethernet address, its IP address, and the IP address of the destination, filling the destination IP Address with 1 and signaling that it is requesting the relevant Ethernet address. The computer owning the address then responds, and the IP packet can then be sent to that Ethernet address.

The ARP protocol is designed to serve in a more general fashion; it includes a Hardware Address Type and a Protocol Address Type that can be set according to the higher-level protocol's needs.

**See Also:** Ethernet; Internet; Internet Protocol (IP); IP Addresses; Packet; Protocol; TCP/IP or Transmission Control Protocol/Internet Protocol.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

**ARP Redirect** (general term): A common tool in a cracker's toolbox, the ARP Redirect literally redirects **Internet** traffic from a local computer through the cracker's **computer**, allowing him or her to "sniff" it (a kind of wiretap that eavesdrops on computer **network**s). The drawback of this form of attack is that the cracker's computer has to be in the same local area network as the computer being attacked. ARP redirects are frequently used by **crackers** as a means of gathering further intelligence from a previously compromised host on the local network.

**See Also:** Computer; Crackers; Internet; Network; Sniffer Program or Packet Sniffer.

**Artificial Intelligence (AI)** (general term): The branch of **computer** science concerned with making computers behave like humans by modelling on computers human thoughts. Sometimes AI is meant to solve a problem that a person can solve but do so more efficiently using a computer.

Coined by Stanford University Professor John McCarthy, AI in recent years has been applied to games-playing programming (by making computers play chess and checkers), expert-systems programming (by making computers help doctors diagnose diseases based on symptoms cited), natural language-programming (by making computers understand natural human languages), neural network-programming (by making computers simulate intelligence by attempting to reproduce various types of physical connections occurring in animal and human brains), and robotic programming (by making computers see, hear, and react to various sensory stimuli).

To date, no computer is able to exhibit "full AI," that is, fully simulating human behavior. The two most common **programming languages** used for AI activities are LISP and Prolog.

**See Also:** Computer; Programming Languages C, C++, Perl, and Java.

**Further Reading:** Free On-Line Dictionary of Computing. Artificial Intelligence. [Online, January 19, 2002.] Free On-Line Dictionary of Computing Website. http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?AI; Jupitermedia Corporation. Artificial Intelligence. [Online, February 10, 2004.] Jupitermedia Corporation Website. http://www.webopedia.com/TERM/a/artificial_intelligence.html.

**Artificial Intelligence Lab** (general term): A very famous place, the MIT Artificial Intelligence (MIT **AI**) Lab has been at the forefront of Artificial Intelligence research since 1959. The primary goal of the AI Lab is to not only understand the nature of intelligence but also engineer **computer** systems exhibiting some form of intelligence. The MIT AI Lab is interdisciplinary in nature and encompasses more than 200 academics across several academic departments. Members of the MIT AI Lab believe that vision, robotics, and language are the critical keys to understanding intelligence. On July 1, 2003, the MIT AI Lab merged with the Lab for Computer Science (LCS) to become the MIT CSAIL (Computer Science and Artificial Intelligence Lab).

**See Also:** Artificial Intelligence (AI); Computer.

**Further Reading:** MIT Artificial Intelligence Lab. MIT Artificial Intelligence Laboratory. [Online, 2004.] MIT Artificial Intelligence Lab Website. http://www.ai.mit.edu/.

**ASCII (American Standard Code for Information Exchange) Character Set** (general term): This character set is utilized to encode characters such as letters, numbers, and punctuation marks, with each character assigned a 7-bit number code.

**Further Reading:** Panda Software. Glossary of Terms. [Online, April 9, 2006.] http://www.pandasoftware.com/virus_info/encyclopedia/glosary.htm#ASCII.

**ASCII (American Standard Code for Information Exchange) Data File** (general term): Stores the values of variables in ASCII format. An ASCII data file is different from a typical word processing file. In particular, a typical word processing file has formatting information such as font size, margin information, and header and footer information. An ASCII data file, in contrast, contains just the values, not the variable definition information. ASCII data files are known as "raw" data files because they have the data but no variable definition information, in contrast to system files, which contain both. An ASCII data file can be made using the text or the DOS text save options in the word processor. Computer programs designed to collect experimental data often store the information collected in ASCII files.

**Further Reading:** Becker, L. Overview of ASCII Data Files. [Online, July 7, 1999.] http://web.uccs.edu/lbecker/SPSS80/ascii.htm.

**ASCII (American Standard Code for Information Exchange) Transfer** (general term): ASCII transfer means sending ASCII information rather than program files, images, and other nontextual information. In contrast, binary transfer means sending program files, images, and other nontextual information.

**Further Reading:** Ziff Davis Media. ASCII Transfer Definition. [Online, April 9, 2006.] http://www.pcmag.com/encyclopedia_term/0,2542,t=ASCII+transfer&i=38023,00.asp.

**Ashcroft, John David** (person; 1942– ): Attorney General of the United States from January 20, 2001, to February 3, 2005. In this role, Ashcroft represented the United States in legal matters, advising the U.S. President and executive department heads. In July 2001, he established the Computer Hacking and Intellectual Property units in the Department of Justice to take an active role in the fight against **cracking** and **cybercrime**.

On November 10, 2004, the White House announced that John Ashcroft would resign his post as soon as a suitable replacement could be named. He was succeeded by Alberto Gonzales.

**See Also:** Cracking, Cybercrime and Cybercriminals, U.S. Department of Justice.

**Further Reading**: King, J. Inside Politics: Evans, Ashcroft Resign from Cabinet. [Online, November 10, 2004.] CNN Website. http://edition.cnn.com/2004/ALLPOLITICS/11/09/cabinet.resignations/. U.S. Department of Justice. Office of the Attorney General. [Online, 2004]. U.S. Department of Justice Website. http://www.usdoj.gov/ag/

**Asia Pacific Network Information Centre (APNIC)** (general term): One of five Regional **Internet** Registries operating globally to register and administer **IP Addresses**, this one serves the Asia Pacific region. It is a not-for-profit organization whose constituents consist of 62 economies and include Internet Service Providers, National Internet Registries, and like organizations. Membership in APNIC gives organizations access to all services, including requests for allocation and registration of IP Address resources as well as registration at specialized training courses. Membership also gives organizations an opportunity to participate in policy development processes and to have voting rights at membership meetings.

**See Also:** Internet; Internet Protocol (IP); IP Addresses.

**Further Reading:** Asia Pacific Network Information Centre. About APNIC: Addressing the Challenge of Responsible Internet Resource Distribution in the Asia Pacific Region. [Online, June 16, 2004.] Asia Pacific Network Information Centre Website. http://www.apnic.net/info/about.html.

**Asynchronous** (general term): Asynchronous refers to transmission of data through networks, and the transmission is not governed by specific timing requirements on the transmission end. Asynchronous transmission is used on a byte level as well as on the level of entire messages.

**See Also:** Bytes.

**Asynchronous Transfer Mode (ATM) and the ATM Forum** (general term): To keep pace with new technological advances (such as video conferencing), the **telecom**munications industry has had to introduce technology that provides a common format for services with different bandwidth requirements. This technology, known as Asynchronous Transfer Mode, or ATM, was initially made for a future network platform of a heterogeneous form—such as broadband-integrated services digital networks (known as B-ISDN). B-ISDN concepts suggest utilizing synchronous optical networks (known as SONET) for long distance or Wide Area Networks (**WANs**).

Asynchronous Transfer Mode is the work of the ATM Forum (ATMF), a group of more than 700 computer suppliers, **network** equipment suppliers, and public carriers. ATM does not use bridge and router devices to connect to remote endpoint devices but instead uses cell switches. As ATM has developed in recent years, it has become a crucial item in assisting companies in their delivery, management, and maintenance of goods and services.

In 1991, the ATM Forum was established to expedite the utilization of ATM products and services through a rapid convergence of interoperability specifications and to promote industry cooperation and market awareness. Currently, the global market for ATM is worth billions of dollars, for with the growth of the **Internet**, the need for broadband access has also increased.

The ATM Forum has in recent years arranged for conferences on such timely topics as Homeland Security and Public Safety Networks, Federal Aviation Administration Network Security, and Mobility for Emergency and Safety Applications.

**See Also:** Internet; Network; Telecom; Wide Area Networks (WAN).

**Further Reading:** QUT Division of Technology, Information and Learning Support. Network Glossary. [Online, July 17, 2003.] QUT Division of Technology, Information and Learning Support Website. http://www.its.qut.edu.au/network/glossary.jsp; The ATM Forum. The History of ATM Technology. [Online, 2002.] The ATM Forum Website. http://www.atmforum.com/aboutatm/history.html.

**Attack** (general term): The term *attack* can be used in a number of ways, from the more general meaning of an attempt by a cracker to break into a computer to deface a home page or to install a virus on a computer to the more technical information security approach of the term, meaning an attack to a cryptosystem. In the latter usage, a security professional is suggesting that a cracker is searching for weaknesses in the computer system that will allow him or her to decrypt encrypted information in that system.

The various types of attacks on computer systems are many and include the following: **passive attacks**, which, when using sniffers, can take place by eavesdropping and may not be detected; **active attacks**, which require some interaction such as altering data and can be detected; remote attacks, which do not occur on-site; a hit-and-run **ping of death attack,** which crashes a computer; a **smurf** or persistent attack, which affects the target's machine for a limited amount of time—and then lets it return to normal; a **replay attack**, which is an active attack whereby the **cracker** tries to capture message parts and then resend a message sometime later with changes; a brute-force attack, which is a fatiguing attempt to try all combinations until a successful break-in occurs; a **man-in-the-middle** attack, which involves either eavesdropping on an existing connection or interposing oneself in the middle of a connection and changing data; a hijack attack, which literally hijacks one side of a connection; and rewrite attacks, which change an encrypted message without first decrypting it.

Targeted attacks that have the goal of taking over control of a computer system typically contain five distinct phases. In the reconnaissance phase, the attacker tries to find potential candidates for an attack; he or she gathers information about the infrastructure of a network, the people involved in using and managing the network, and the computers attached to it. The second phase includes a scan of the system or a range of systems for vulnerabilities. In the third phase, the **vulnerabilities** are exploited, either by gaining access to the system or denying service to it. In the fourth phase, the attacker uses a variety of methods to gain access by installing a **back door** listener, a **RootKit**, or a **Kernel**-level RootKit. The last phase of an attack typically involves the attacker's covering his or her tracks so that the administrator of a computer system would find it difficult to detect that the system has been compromised.

**See Also:** Active Attacks; Back or Trap Door; Cracker; Kernel; Man-in-the-Middle Attack; Passive Attacks; Ping of Death Attack; Replay Attack; RootKit; Smurf; Vulnerabilities of Computers.

**Further Reading:** Graham, R. Hacking Lexicon. [Online, 2001.] Robert Graham Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

**Audit Trail** (general term): An auditing subsystem within an enterprise that monitors actions and keeps a record of every user **logging in** to the system.

**See Also:** Logging In.

**Audits and Alarm Classification** (general term): To determine whether their **computer** systems are secure, businesses, government agencies, and medical and educational institutions often maintain the services of computer **security** professionals to conduct a security audit—a validation of an enterprise's security profile, with details on "alarm classifications." This type of security audit is not much different from accounting audits that review a company's financial profile and books.

Most information detected in security audits relates to breaches in the system because of the rather harmless curiosity of neophyte crackers—or honest mistakes by organizational insiders. However, as security experts advise, harmless or not all incidents need to be logged and reported in a statistical summary. This summary can then be analyzed by computer security professionals to find suspicious cyber activities and to classify the severity of incidents. Common **incident**s that are terminated by regular security measures—such as an unsuccessful attempt by a cracker to **telnet** to the enterprise's **firewall** system—should be recorded but not typically noted as "a severe incident." In contrast, activities indicating that a successful attack is in progress—such as the unexpected alteration of an executable file—should be reported immediately and logged as "an incident of concern."

Alarm classification requires an acute combination of experience on the job by the security expert and common sense. In general, when a security expert is in doubt about how to note incidents, the advice given by senior experts in the field is to overclassify rather than underclassify an incident. Note, however, that in one enterprise, an unsuccessful telnet attempt from an unknown **host** to the firewall may be unimportant, whereas in another enterprise such as a bank, this type of incident may be considered critical and requiring immediate attention from the system administrator.

A revealing news story surfacing in the U.K. on May 19, 2005, claimed that some U.K. financial institutions ignore the findings of security audits and just treat audits as a necessary legal step to satisfy corporate governance regulations. A managing consultant at Integralis maintained that financial institutions are told that they have to carry out a penetration test to comply with audits, but in about 5% of the cases reviewed, the security team continues to find the same system faults audit after audit. Though in some cases the financial institutions claim a lack of resources to correct the discovered flaws, often it is a matter of misplaced priorities; getting new applications up and running is too often their top priority, leaving uncovered security flaws lower on the priority list.

**See Also:** Computer; Firewall; Host; Incident; Incident Response; Security, Telnet.

**Further Reading:** Leyden, J. U.K. Banks Ignore Security Audit Findings. Reg SETI Group Website. http://www.theregister.co.uk/2005/05/19/audit_ignoramuses/; Pipkin, D.L. *Halting the Hacker: A Practical Guide to Computer Security*. Upper Saddle River, NJ: Prentice Hall, 2003.

**Australian Defence Signals Directorate (DSD**) (general term): Australia's authority regarding signals **intelligence** and information security. The DSD has two primary functions: to collect and disseminate foreign signals intelligence (called Sigint) and to provide Information security (Infosec) services and products to the government and its Defence force. Though the DSD's information security role is not classified information, the Directorate's foreign signals intelligence role is, to a great degree, classified information.

**See Also:** Intelligence.

**Further Reading:** Defence Signals Directorate. Welcome to the Website of the Defence Signals Directorate. [Online, May 14, 2004.] Defence Signals Directorate Website. http://www.dsd.gov.au/.

**Authentication** (general term): The process of identifying an individual, message, file, and other data. The two major roles for authentication, therefore, are as follows: (1) confirming that the user is who he or she claims to be; and (2) that the message is authentic and not altered or forged. The term *authentication* should not be confused with a closely related term, ***authorization***, which means determining what a user is allowed to do or see.

In recent years, a number of products have been developed to assist in the authentication process, including biometrics (assessing users' signatures, facial features, and other biological identifiers); smart cards (having microprocessor chips that run cryptographic **algorithms** and store a private key); digital certificates containing public or private **keys**; and **SecureID**, a commercialized product using a key and the current time to generate a random numbers stream that is verifiable by a server—thus ensuring that a potential user puts in the number on the card within a set amount of time (typically 5 or 10 seconds).

**See Also:** AAA; Algorithm; Authorization; Key; SecureID.

**Further Reading:** Graham, R. Hacking Lexicon. Robert Graham Website. http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html.

**Authenticity** (general term): A close relative of **authentication**, authenticity is the process of ensuring that a message received is the same message that was sent and has not been tampered with or altered. Lawyers, as a real-world case in point, are fanatical about ensuring that evidence is authentic and has not been tampered with or altered in any way to ensure a fair hearing for the accused. This is called chain of custody and is a critical concept in reference to cybercrime.

**See Also:** Authentication.

**Authorization** (general term): Determining what a user is allowed to do on a **computer** system or software application is known as authorization. In the world of Web applications, authorization is bidirectional, meaning that it controls what a user can do and also what a user can get in return from the application.

**See Also:** Computer.

**Autoencryption (virus)** (general term): How a virus encrypts—or codifies—all or part of itself. When this occurs, a virus scanner or an analyst will find it more difficult to detect or to analyze.

**Further Reading:** Wickham Enterprises. Multi-Function Printer.com. [Online, 2005.] http://www.multifunction-printer.com/virus_glossary/.

**Availability** (general term): One of the critical missions of the system **administrator**; that is, to ensure that the computer system not only is available to users 24 hours per day, every day, but also is secure. A system that is shut down may be secure because crackers cannot enter it and do their damage, but the cost to the enterprise can be extreme in terms of lost productivity and sales. For this reason, system administrators act expeditiously in the event of a **Denial of Service** (**DoS**) attack. Some safety features are built into secure systems that actually force a shutdown, including fail-close/fail-open, whereby a system shuts down when security features are compromised, such as when a **firewall** crashes. Another example is account lockouts, which occur when a computer system encounters an onslaught of "bad" **password**s, thus locking out the accounts in question.

**See Also:** Administrator; Denial of Service (DoS); Firewall; Password; Webmaster.

**Axis of Evil or Terrorist-Sponsoring Nations** (general term): Dubbed "the axis of evil" by President George W. Bush, as of 2002, the United States Department of State has listed what the United States deems to be seven designated state sponsors of **terrorism**: Cuba, Iran, Iraq, North Korea, Libya, Syria, and Sudan. According to the U.S. government, these countries have been identified as sponsoring terrorist organizations and providing them with weapons and high-technology products for plotting and executing their violent operations against targeted nations.

**See Also:** Internet; Terrorism; Terrorist-Hacker Links; Cyberwarfare.

**Further Reading:** Wilson, C. CRS Report for Congress: Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. [Online, October 17, 2003.] CRS Report Website. http://www.fas.org/irp/crs/RL32114.pdf.