

Security Acronyms & Terms

Acronym	Term Name	Definition / Information
3DES	Triple DES	Data Encryption Standard – another mode of DES operation based on the DES algorithm. Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES.
3G	Third generation	3G refers to the third generation of developments in wireless technology, especially mobile communications. The third generation, as its name suggests, follows the first generation (1G) and second generation (2G) in wireless communications. The 1G period began in the late 1970s and lasted through the 1980s. These systems featured the first true mobile phone systems, known at first as "cellular mobile radio telephone."
Algorithms	Algorithms	A step-by-step procedure for solving a problem or accomplishing some end especially by a computer.
ASR	Automatic Speech Recognition	The process of converting a speech signal to a set of words, by means of an algorithm implemented as a computer program.
AV	Anti-Virus Software	Commonly known as AV scanners, which detect and eliminate viruses from computer systems.
BB	Broadband	A transmission method in which the network's range of transmission frequencies is divided into separate channels and each channel is used to send a different signal. Broadband is often used to send different types of signals simultaneously.
BCP	Business Continuity Plan	A methodology used to create a plan for how an organization will resume partially or completely interrupted critical function(s) within a predetermined time after a disaster or disruption. BCP may be a part of a larger organizational effort to reduce operational risk associated with poor information security controls, and thus has a number of overlaps with the practice of risk management.
Bio	Biometrics	The measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity.
Cache	Cache	A special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Acronym	Term Name	Definition / Information
CGI	Common Gateway Interface	The Common Gateway Interface (CGI) is a standard for interfacing external applications with information servers, such as HTTP or Web servers. A CGI program is executable; it is basically the equivalent of letting the world run a program on your system, which isn't the safest thing to do. Therefore, there are some security precautions that need to be implemented when it comes to using CGI programs.
CPE	Customer Premise Equipment	Any terminal, associated equipment, and inside wiring located on the subscriber's premises that connect with a telecommunications channel.
DES	Data Encryption Standard	Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It has widespread use internationally.
DHA	Directory Harvest Attacks	A method to learn valid e-mail addresses.
DHCP	Dynamic Host Configuration Protocol	Dynamic Host Configuration Protocol (DHCP) is a protocol used by computers to obtain unique IP address, default router, subnet mask, and IP addresses for DNS servers from DHCP servers. This protocol is used when a computer (especially notebook) is added to a network.
DNS	Domain Name System	An Internet service that translates domain names into IP addresses.
DNS	Domain Name Service	An Internet service that allows us to use symbolic names (e.g. www.ukorbit.com) instead of a numerical IP address when contacting computers connected to the Internet.
DR	Disaster Recovery	Every business and organization can experience a serious incident which can prevent it from continuing normal operations. The potential causes are many and varied: flood, explosion, computer malfunction, accident, grievous act... the list is endless. A DRP can help you reduce both the risk and impact should the worst occur.
DSL	Digital Subscriber Line	DSL is a very high-speed connection that uses the same wires as a regular telephone line. A DSL connection manages to squeeze more information through a standard phone line – and lets you make regular telephone calls even when you're online.
EH	Ethernet Hub	A device for combining multiple Ethernet segments (typically 10BaseT) into a single segment. All traffic appearing on any port of a hub will be echoed to all of the other ports instantaneously.

Acronym	Term Name	Definition / Information
ES	Ethernet Switch	A device for connecting multiple Ethernet segments, while maintaining them as separate segments. Unlike a hub, a switch will intelligently route packets to the appropriate port (only) based on the MAC-level (OSI Layer 2) address in the packet.
ESP	Electronic Satellite Pursuit	GPS/GSM based tracking system that provides law enforcement agencies with tracking data to quickly and accurately locate a position.
FFIEC	Federal Financial Institutions Examination Council	The Council is a formal interagency body empowered to prescribe uniform principles.
FINCEN	Financial Crimes Enforcement Network	Safeguards the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity.
Firewall	Firewall	Hardware and/or software used to prevent computer hackers from getting into a computer system.
FTP	File Transfer Protocol	A protocol that allows the transfer of files from one computer to another over the Internet.
GLBA	Gramm-Leach-Bliley Act	An act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies, and insurance companies. The Gramm-Leach-Bliley Act (GLBA) allowed commercial and investment banks to consolidate.
GPS/GSM	Global Positioning System	The Global Positioning System, usually called GPS, is the only fully functional satellite navigation system. The Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world.
GUI	Graphical User Interface	Interface that organizes and presents information in a format that is easy to read and interpret.
Hackers	Hackers	A hacker is a person who, by evading security measures, creates and modifies computer software and computer hardware, including computer programming, administration, and security-related items.
HIDS	Host-Based Intrusion Detection System	A Host-Based Intrusion Detection System (HIDS), as a special category of an Intrusion-Detection System, focuses its monitoring and analysis on the internals of a computing system rather than on its external interfaces (as a Network Intrusion Detection System (NIDS) would do).
HIPS	Host-Based Intrusion Prevention System	One of the newer technologies is the IPS – Intrusion Prevention System. An IPS is somewhat like combining an IDS with a firewall. A typical IDS will log or alert you to suspicious traffic.

Acronym	Term Name	Definition / Information
HTML	Hypertext Markup Language	The basic language to write web pages.
HTTP	Hypertext Transfer Protocol	The protocol for moving hypertext files across the Internet which allows you to view web pages in a browser.
Hyperlink	Hyperlink	A word, button, or graphic on a web page that opens a different page in a web browser when clicked with a mouse.
IDS / IPS	Intrusion Detection/ Prevention System	When you combine the blocking capabilities of a firewall with the deep packet inspection of an IDS, you get the new kid on the block: intrusion prevention systems or IPS. Any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful is an IDS.
IMAP	Internet Message Access Protocol	The Internet Message Access Protocol (commonly known as IMAP or IMAP4, and previously called Internet Mail Access Protocol) is an application layer Internet protocol that allows a local client to access e-mail on a remote server.
IP	Internet Protocol	The transport protocol used on the Internet and many private networks.
IPSec	IP Security Architecture	A proposed Internet standard for providing security services at the IP layer level. Some early implementations exist, for example in Cisco routers.
IRC	Internet Relay Chat	An Internet protocol that allows people to meet in conference groups (called channels) and chat with each other by typing.
ISDN	Integrated Services Digital Network	A telecommunications standard that uses digital technology to support voice, video, and data communications over regular telephone lines.
Kerberos	Kerberos	An authentication protocol employing "tickets" generated with private key encryption to authorize transactions between a user and a remote server.
L2TP	Layer 2 Tunneling Protocol	An emerging standard for "tunneling" a variety of protocols across an IP connection. It is being forged as a compromise between Cisco's Layer 2 Forwarding (L2F) and Microsoft's (et al) PPTP.
LAN	Local Area Network	A local area network (LAN) is a computer network covering a small local area, like a home, office, or small group of buildings such as a home, office, or college. Current LANs are most likely to be based on switched Ethernet or Wi-Fi technology running at 10, 100 or 1,000 Mbit/s. The defining characteristics of LANs in contrast to WANs (wide area networks) are: their much higher data rates; smaller geographic range; and that they do not require leased telecommunication lines.

Acronym	Term Name	Definition / Information
Modem	Modem	The word “modem” is a contraction of the words modulator-demodulator. A modem is typically used to send digital data over a phone line. The sending modem modulates the data into a signal that is compatible with the phone line, and the receiving modem demodulates the signal back into digital data. Wireless modems convert digital data into radio signals and back.
MSSP	Managed Security Service Provider	An MSSP (managed security service provider) is an Internet service provider (ISP) that provides an organization with some amount of network security management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and virtual private network (VPN) management. An MSSP can also handle system changes, modifications, and upgrades.
MITM	Man in the Middle	An attack in which an attacker is able to read, insert, and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. MITM is typically used to refer to active manipulation of the messages, rather than passively eavesdropping.
NAS	Network Access Server	Acts as a gateway to guard access to a protected resource from anything to telephone network, to printer or to the Internet.
NAT	Network Address Translation	In computer networking, the process of network address translation (NAT, also known as network masquerading or IP-masquerading) involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address (see gateway).
NIDS/NIPS	Network Based Intrusion	An intrusion detection system (IDS) monitors network traffic Detection/Protection System and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.
NP	Nonrepudiation	In reference to digital security, nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.
OSSTMM	Open Source Security Testing Methodology Manual	OSSTMM provides a methodology for a thorough security test. A security test is an accurate measurement of security at an operational level, void of assumptions and anecdotal evidence. A proper methodology makes for a valid security measurement which is consistent and repeatable. An open methodology means that it is free from political and corporate agendas. An open

Acronym	Term Name	Definition / Information
		source methodology allows for free dissemination of information and intellectual property. This is the OSSTMM. It is the collective development of a true security test and the extraction of factual security metrics.
Phishing	Phishing	Sending an e-mail to a user and falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.
Pharming	Pharming	Pharming is a hacker's attack aiming to redirect a Web site's traffic to another (bogus) Web site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.
Portal		A protocol to sending e-mail messages between servers.
POP	Post Office Protocol	In computing, local e-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. Nearly all subscribers to individual Internet service provider e-mail accounts access their e-mail with client software that uses POP3.
POTS	Plain Old Telephone System (see also PSTN)	A commonly used acronym for dial-up analog telephone lines.
PPP	Point to Point Protocol	In computing, the Point-to-Point Protocol, or PPP, is commonly used to establish a direct connection between two nodes. It can connect computers using serial cable, phone line, trunk line, cellular telephone, specialized radio links, or fiber optic links. Most Internet service providers use PPP for customers' dial-up access to the Internet.
PPTP	Point-to-Point Tunneling Protocol	A standard developed jointly by Microsoft, U.S. Robotics, 3Com, and others, for tunneling PPP packets across IP connections. This protocol, incorporated into Windows NT, Windows 95/98, and other products, is now being merged with Cisco's Layer 2 Forwarding (L2F) into a new Internet standard called Layer 2 Tunneling Protocol (L2TP).
Proxy	Proxy	A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. A proxy server can also serve as a firewall.

Acronym	Term Name	Definition / Information
PSTN	Public Switched	Typically refers to common dial-up telecommunications, often Telephone Network extended to include ISDN.
RAS	Remote Access Server	A server that is dedicated to handling users that are not on a LAN but need remote access to it.
Router		A device for intelligently switching traffic between multiple networks, based on a stored configuration and sophisticated routing software. Routers can switch traffic based on either MAC-level (OSI Layer 2) or Protocol-level (OSI Layer 3) addresses. These capabilities allow routers to perform security functions, as well as adaptive network reconfiguration.
SAR	Suspicious Activity Report	A Suspicious Activity Report (or SAR) is a report regarding suspicious or potentially suspicious financial activity, filed with the Financial Crimes Enforcement Network (FinCEN), an agency of the United States Department of the Treasury.
SAS70	SAS70	Auditing standards – an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants. Requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.
SLA	Service Level Agreement	Service Level Agreement (SLA) is a formal written agreement made between two parties: the service provider and the service recipient. It is a core concept of IT Service Management.
SMTP	Simple Mail Transfer Protocol	The main protocol used to send e-mail from server to server on the Internet developed by Netscape for transmitting private documents.
Sniffer		A “sniffer” is a program that is surreptitiously installed on a computer within a local network. The purpose of the program is to put the computer’s network interface into “promiscuous mode” (yes, it’s really called that), so that it will receive every packet that appears on the network. The sniffer creates a log file on the computer’s disk containing this network data, which may later be retrieved by the perpetrator and analyzed for information such as passwords or proprietary information.
SPAM	Spam	Common name for UCE (unsolicited commercial e-mail).
SPARC	Scalable Processor Architecture	Is a 32 and 64 bit microprocessor architecture from Sun Microsystems that is based on reduced instruction set computing (RISC).
SSL	Secure Sockets Layer	A protocol to sending email messages between servers.
TCP/IP	Transmission Control Protocol/Internet Protocol	The protocols which enable the transfer of files to and from servers and computers over the Internet.

Acronym	Term Name	Definition / Information
Trojan	Trojan	A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.
UPnP	Universal Plug and Play	UPnP is a standard that enables various devices to plug into a network and automatically know about each other.
URL	Uniform Resource Locator	The address of a Web site (e.g. www.ukorbit.com) or other Internet resource.
UTM	Unified Threat Management	Appliances have AV, IDS/IPS, content filtering, spam filtering and firewall in one box. Sits at gateway right behind the router. Layer 2 to layer 7.
Virus	Virus	Destructive computer program spread between computers.
VLAN	Virtual Local Area Network	A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).
VPDN	Virtual Private Dial-up Network	A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) from a remote user across an ISP network to a private network. VPDNs are a cost effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.
VPN	Virtual Private Network	A term typically used to refer to the creation of a protected network channel over public networking conduits such as the Internet. Technologies used to create VPNs include L2TP and PPTP.
VRS	Voice Recovery Systems	A system to route your business calls to any destination ensuring your phone service is restored with minimal interruption in the case of an emergency. Business Continuity Plan (BCP) specific to your organization should require phone routing capabilities and service compliance.
WAN	Wide Area Network	A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.