TEXAS STATE LIBRARY & ARCHIVES COMMISSION WEB SITE
Agency Info | General Interest | Librarians | Govt Agencies | Catalogs & Searches | Publications | News | TRAIL

Texas State Library and Archives Commission
Making Information Work for All Texans

Services to Librarians > Resources for Librarians

Glossary

The terms presented in this glossary are taken from DigitalGuards☐ terminology database. I am grateful for Gregory L. Stockdale☐s permission to reproduce them here. You can find the most recently updated version of the terminology database at **http://www.digitalguards.com/Glossary.htm**. You will also find databases of network security tools and other information at the DigitalGuards web site.

Active Attack
An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files.

Administrative Security
The management constraints and supplemental controls established to provide an acceptable level of protection for data.

AIS
Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Alert
A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.

Ankle-Biter
A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AIS's. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet.

Application Level Gateway
(Firewall) A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Assessment
Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Assurance
A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Attack
An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit
The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail
In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authenticate
To establish the validity of a claimed user or object.

Authentication
To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Automated Security Monitoring
All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive, unclassified or critical data, material, or processes in the system.

Availability
Assuring information and communications services will be ready for use when expected.

Back Door
A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Breach
The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Buffer Overflow
This happens when more data is put into a buffer or holding area, then the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.

Bug
An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.

CGI
Common Gateway Interface - CGI is the method that Web servers use to allow interaction between servers and programs.

CGI Scripts
Allows for the creation of dynamic and interactive web pages. They also tend to be the most vulnerable part of a web server (besides the underlying host security).

Circuit Level Gateway
One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

COAST
Computer Operations, Audit, and Security Technology - is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Its research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems.

Compromise
An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred.

Computer Abuse
The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.

Computer Fraud
Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack
(CAN) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DODD S-3600.1 of 9 Dec 96)

Computer Security
Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Computer Security Incident
Any intrusion or attempted intrusion into an automated information system (AIS). Incidents can include probes of multiple computer systems.

Computer Security Intrusion
Any event of unauthorized access or penetration to an automated information system (AIS).

Confidentiality
Assuring information will be kept secret, with access limited to appropriate persons.

Countermeasures
Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.

Crack
A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.

Cracker
One who breaks security on an AIS.

Cracking
The act of breaking into a computer system.

Crash
A sudden, usually drastic failure of a computer system.

Cryptography
The art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cyberspace
Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.

Dark-side Hacker
A criminal or malicious hacker.

DARPA
Defense Advanced Research Projects Agency.

Data Driven Attack
A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard
Definition 1) (DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use. Definition 2) A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Demon Dialer
A program which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a denial of service attack.

Denial of Service
Action(s) which prevent any part of an AIS from functioning in accordance with its intended purpose.

Derf
The act of exploiting a terminal which someone else has absent-mindedly left logged on.

DES
See *Data Encryption Standard*

DMZ
Demilitarized Zone - A part of the network that is neither part of the internal network nor directly part of the Internet. Basically a network sitting between two networks.

DNS Spoofing
Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for

a valid domain.

Encapsulating Security Payload
(ESP) A mechanism to provide confidentiality and integrity protection to IP datagrams.

Ethernet Sniffing
This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like login or password.

False Negative
Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

False Positive
Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

Fault Tolerance
The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Firewall
A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

Fishbowl
To contain, isolate and monitor an unauthorized user within a system in order to gain information about the user.

Hacker
A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn on the minimum necessary.

Hacking
Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Hacking Run
A hack session extended long outside normal working times, especially one longer than 12 hours.

Host
A single computer or workstation; it can be connected to a network.

Host Based
Information, such as audit data from a single host which may be used to detect intrusions.

IDEA
(International Data Encryption Algorithm) - A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key.

IDIOT
Intrusion Detection In Our Time. A system that detects intrusions using pattern-matching.

Integrity
Assuring information will not be accidentally or maliciously altered or destroyed.

Internet Worm
A worm program (see: Worm) that was unleashed on the Internet in 1988. It was written by Robert T. Morris as an experiment that got out of hand.

Intrusion
Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection
Pertaining to techniques which attempt to detect intrusion into a computer or

network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Splicing / Hijacking
An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP Spoofing
An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

Key
A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.

Key Escrow
The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

Keystroke Monitoring
A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

LAN
Local Area Network - A computer communications system limited to no more than a few miles and using high-speed connections (2 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including workstations, front-end processors, controllers, switches, and gateways.

Leapfrog Attack
Use of userid and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letterbomb
A piece of e-mail containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

Mailbomb
The mail sent to urge others to send massive amounts of e-mail to a single system or person, with the intent to crash the recipient's system. Mailbombing is widely regarded as a serious offense.

Malicious Code
Hardware, software, of firmware that is intentionally included in a system for an unauthorized purpose; e.g. a Trojan horse.

Metric
A random variable x representing a quantitative measure accumulated over a period.

Mockingbird
A computer program or process which mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Multihost Based Auditing
Audit data from multiple hosts may be used to detect intrusions.

Nak Attack
Negative Acknowledgment - A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus, leaves the system in an unprotected state during such interrupts.

Network
Two or more machines interconnected for communications.

Network Based
Network traffic data along with audit data from the hosts used to detect intrusions.

Network Level Firewall
A firewall in which traffic is examined at the network protocol (IP) packet level.

Network Security
Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

Network Security Officer
Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

Non-Repudiation
Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Open Security
Environment that does not provide environment sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

Open Systems Security
Provision of tools for the secure internetworking of open systems.

Operational Data Security
The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Operations Security
Definition 1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. Definition 2) An analytical process by with the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

Orange Book
See Trusted Computer Security Evaluation Criteria.

OSI
Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

Packet
A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Filter
Inspects each packet for user defined content, such as an IP address but does not track the state of sessions. This is one of the least secure types of firewall.

Packet Filtering
A feature incorporated into routers and bridges to limit the flow of information based on predetermined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.

Packet Sniffer
A device or program that monitors the data traveling between computers on a network.

Passive Attack
Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

Passive Threat
The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

PEM (Privacy Enhanced Mail)

An IETF standard for secure electronic mail exchange.

Penetration
The successful unauthorized access to an automated system.

Penetration Signature
The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.

Penetration Testing
The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

Perimeter Based Security
The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

Perpetrator
The entity from the external environment that is taken to be the cause of a risk. An entity in the external environment that performs an attack, i.e. hacker.

Personnel Security
The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

PGP (Pretty Good Privacy)
A freeware program primarily for secure electronic mail.

Phage
A program that modifies other programs or databases in unauthorized ways; especially one that propagates a virus or Trojan horse.

PHF
Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF hack
A well-known and vulnerable CGI script which does not filter out special characters (such as a new line) input by a user.

Phracker
An individual who combines phone phreaking with computer hacking.

Phreak(er)
An individual fascinated by the telephone system. Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another.

Phreaking
The art and science of cracking the phone network.

Physical Security
The measures used to provide physical protection of resources against deliberate and accidental threats.

Piggy Back
The gaining of unauthorized access to a system via another user's legitimate connection.

Ping of Death
The use of Ping with a packet size higher than 65,507. This will cause a denial of service.

Plaintext
Unencrypted data.

Private Key Cryptography
An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group.

Probe
Any effort to gather information about a machine or its users for the apparent purpose of gaining unauthorized access to the system at a later date.

Procedural Security

Procedural Security
See Administrative Security.

Profile
Patterns of a user's activity which can detect changes in normal routines.

Promiscuous Mode
Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffer), regardless of its destination.

Protocol
Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

Proxy
A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Public Key Cryptography
Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

Red Book
See Trusted Network Interpretation.

Replicator
Any program that acts to produce copies of itself examples include; a program, a worm, a fork bomb or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

Retro-Virus
A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Risk Assessment
A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management
The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval.

Rootkit
A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

Router
An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Routing Control
The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.

RSA Algorithm
RSA stands for Rivest-Shamir-Aldeman. A public-key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult.

Rules Based Detection
The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system

vulnerabilities. Also known as Misuse Detection.

Samurai
A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

SATAN
Security Administrator Tool for Analyzing Networks - A tool for remotely probing and identifying the vulnerabilities of systems on IP networks. A powerful freeware program which helps to identify system security weaknesses.

Script Kiddies
See *Ankle Biters*

Secure Network Server
A device that acts as a gateway between a protected enclave and the outside world.

Secure Shell
A completely encrypted shell connection between two machines protected by a super long pass-phrase.

Security
A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Security Architecture
A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Audit
A search through a computer system for security problems and vulnerabilities.

Security Countermeasures
Countermeasures that are aimed at specific threats and vulnerabilities or involve more active techniques as well as activities traditionally perceived as security.

Security Domains
The sets of objects that a subject has the ability to access.

Security Features
The security-relevant functions, mechanisms, and characteristics of AIS hardware and software.

Security Incident
Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Kernel
The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Officer
The ADP official having the designated responsibility for the security of and ADP system.

Security Perimeter
The boundary where security controls are in effect to protect assets.

Security Policies
The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model
A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security Requirements
Types and levels of protection necessary for equipment, data, information, applications, and facilities.

Security Service
A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Violation
An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

Server
A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.

Simple Network Management Protocol (SNMP)
Software used to control network communications devices using TCP/IP.

Smurfing
A denial of service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim thereby clogging its network.

Snarf
To grab a large document or file for the purpose of using it with or without the author's permission.

Sneaker
An individual hired to break into places in order to test their security; analogous to tiger team.

Sniffer
A program to capture data across a computer network. Used by hackers to capture user id names and passwords. Software tool that audits and identifies network traffic packets. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

Spam
To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

Spoofing
Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to an AIS by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

SSL (Secure Sockets Layer)
A session layer protocol that provides authentication and confidentiality to applications.

Subversion
Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

SYN Flood
When the SYN queue is flooded, no new connection can be opened.

TCP/IP
Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

tcpwrapper
A software tool for security which provides additional network logging, and restricts service access to authorized hosts by service.

Term Rule-Based Security Policy
A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Terminal Hijacking
Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O while a user is on the terminal.

Threat
The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

violation of security.

Threat Agent
Methods and things used to exploit a vulnerability in an information system, operation, or facility; fire, natural disaster and so forth.

Threat Assessment
Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Tiger
A software tool which scans for system weaknesses.

Tiger Team
Government and industry - sponsored teams of computer experts who attempt to break down the defenses of computer systems in an effort to uncover, and eventually patch, security holes.

Tinkerbell Program
A monitoring program used to scan incoming network connections and generate alerts when calls are received from particular sites, or when logins are attempted using certain ID's.

Topology
The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

Trace Packet
In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element.

Traceroute
An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

Tripwire
A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

Trojan Horse
An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Computer System Evaluation Criteria
(TCSEC) A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base (TCB)
The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

Trusted Network Interpretation
The specific security features, the assurance requirements and the rating structure of the Orange Book as extended to networks of computers ranging from isolated LANs to WANs.

TTY Watcher
A hacker tool that allows hackers with even a small amount of skill to hijack terminals. It has a GUI interface.

Vaccines
Program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

Virus
A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability
Hardware, firmware, or software flow that leaves an AIS open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or

could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Analysis
Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

WAN
Wide Area Network. A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

War Dialer
A program that dials a given list or range of numbers and records those which answer with handshake tones, which might be entry points to computer or telecommunications systems.

Worm
Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

return to top

home   contact   site index   policies & disclaimers

SITE NAVIGATION TEXT LINKS
Agency Info | General Interest | Librarians | Govt Agencies | Catalogs & Searches
Our Publications | News | TRAIL | Texas State Library Home Page
Contact Us | Site Index | Policies & Disclaimers | Webmaster