

Computer System Security: A Primer

By J. Craig Lowery, Ph.D.

Computer system security attacks are one of the most urgent problems facing IT professionals today. Security threats challenge administrators to protect their systems without hindering client access. This article provides an overview of current security threats, including the motivations and methods of attackers, the vulnerabilities they exploit, and the defenses administrators employ.

The terms computer virus, hacker, and script kiddy have become part of the common lexicon, illustrating the pervasiveness of computer security issues. Disturbing reports of unauthorized system entry, denial of service, and information theft occur often enough to damage the public trust in computer and network security. These security threats force IT administrators to not only monitor and defend their systems, but also to reassure users that the services they depend on and the data they

entrust to those services are available, intact, and protected from unauthorized access.

The most effective way for administrators to prevent and combat future security attacks is to understand commonalities of past attacks. To do this, administrators should be familiar with attack terminology, which falls into four categories: attacker types, attack goals, exploited vulnerabilities, and defenses against attacks. These four categories provide an excellent structure for studying computer system security at a high level (see Figure 1).

Please note that in the context of this article, the term computer system includes hardware, software, network transmission paths, and people who interact with these components. By this definition, everything from a desktop workstation to the Internet qualifies as a computer system.

Types of computer system attackers

An attacker is a person who tries to gain an advantage by exploiting a security hole. Attackers are misfeasors, masqueraders, or clandestine users.

Misfeasors. These authorized users gain additional but unauthorized access to resources on a system or otherwise misuse their authorization. Examples include programmers who use their accounts to exploit operating system (OS) vulnerabilities and gain administrative privileges, or accountants who embezzle money by falsifying records in a database to which they have regular access.

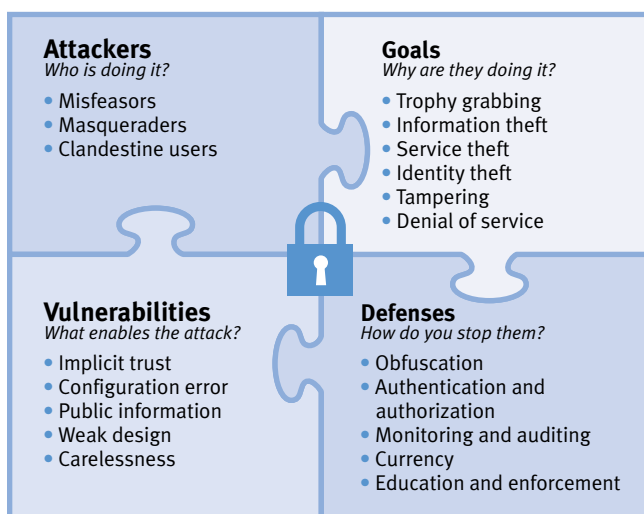


Figure 1. Pieces of the security puzzle

A misfeasor is an “inside” person, someone within an organization who introduces a security risk or poses a threat.

Masqueraders. These people use authorized user access privileges to enter a system and then, posing as that user, attack the system. Examples include hackers who obtain usernames and passwords by cracking password files, and then use that information to gain entry to the system. Masqueraders are usually persons outside the organization.

Clandestine users. These individuals are insiders or outsiders who obtain their own, distinct unauthorized access to a system. Examples include hackers who obtain administrative access to a system long enough to create their own user accounts for subsequent access.

The concepts of access and authorization are not necessarily limited to user accounts within an OS. Physical access to an equipment closet or authorization to place orders for new telephony service are examples of other types of access and authorization. All persons who have any degree of physical or logical interaction with a system, its components, or its processes are capable of compromising system security.

COMMON SECURITY TERMS

Authentication: Verification that a communicating entity owns the identity it claims

Authorization: Determination of access privileges based on identity

CERT/CC: The CERT® Coordination Center (formerly the Computer Emergency Response Team) at Carnegie Mellon University, which specializes in categorizing and investigating computer security threats (see <http://www.cert.org>)

Cleartext: Data in its native, unencrypted form

Cracker: Historically, a person who breaks into computer systems illegally, a meaning now subsumed by hacker

Cyphertext: Data in an encrypted form

Hacker: Historically, a person who studies and manipulates a computer system to probe its abilities, but has now come to connote a miscreant (see also cracker)

Privacy: Guaranteed secrecy of a computer network communication

Security: Protection of a computer or network system from damage or violation from an unauthorized source

Spam: Unsolicited e-mail

Warez: Pirated software downloaded by a hacker

The most effective way
for administrators to
prevent and combat future
security attacks is to
understand commonalities
of past attacks.

Common goals of security attackers

The goals of an attacker range from innocuous to severely damaging:

Trophy grabbing. Most thrill-seeking attackers are trophy grabbing. Their intent is not to disrupt or damage a system, but to prove that they can enter the system. Such accomplishments are badges of achievement in the hacker community.

Information theft. The most common goal of a security attack is information theft. Intruders seek sensitive information such as credit card numbers, usernames, passwords, and medical records.

Service theft. This type of attack involves attackers who use computer resources without paying for them. Software pirates who crack systems to host stolen software, or warez, for others to download are guilty of service theft. Clandestine users also commit service theft by having unauthorized accounts on a server.

Identity theft. This is the act of illegally assuming the identity of another person, or masquerading, to gain control of that person’s resources (usually computer and economic privileges). An example of this is an attacker who uses stolen social security numbers and credit histories to establish and exercise unauthorized lines of credit. Identity theft does not necessarily involve information theft. For example, an attacker can commit e-mail forgery without stealing sensitive information about the e-mail address owner.

Tampering. This attack is more serious than information theft because the attacker alters data rather than simply copying it. A student who changes a grade in a university registrar’s database is tampering. This example is stealthy tampering—the attack is not intended to draw attention. A more extreme form of tampering is defacement, in which a hacker alters a system in a very noticeable way, usually to make a personal or political statement. The disgruntled computer operator who, upon dismissal, embeds nasty messages about management in a login script, or the activist group that hacks into a corporate Web site are typical examples.

Denial of service (DoS). DoS can be the most damaging type of security attack. It diminishes server capacity for authorized clients and temporarily disrupts access to the system. In the worst cases, DoS attacks render a system unusable for a protracted period by destroying not only its ability to communicate, but also any data that has been entrusted to it. DoS also can occur as an unintentional side effect of service theft. For example, hosting pirated warez can bring down a system because of the excessive download activity.

COMMON ATTACKS

Backdoor: A change made to a violated system to make future re-entry easier for the hacker

Bacteria: A program that quickly allocates system resources and reproduces instances of itself to deny service to other processes (also known as hogs)

Buffer overrun: An attack that forces a processor to execute foreign code in privileged mode by passing a lengthy string parameter containing the code to a subroutine that does not have the buffer space to receive it

Compromised system utilities: Common system commands or programs altered by a hacker so that the system extends unintended privileges to unauthorized users, provides a backdoor for later re-entry, or fails to report hacker activities

DNS hijack: An attack that alters the Domain Name System (DNS) so that a DNS lookup for a computer name returns an unintended IP address

E-mail forgery: An attack that constructs e-mail messages to appear as if originating from another person or source

E-mail relay: An attack that bounces messages into a spam-filtering mail system through an unsuspecting, third-party mail system that is not on the filtering list

IP spoofing: A form of masquerading in which the sender of an Internet data packet forges the originating IP address so that the packet appears to have been sent by another system

Keystroke monitoring: Using a hardware or software mechanism to capture user keyboard strokes and report the strokes to a hacker

Logic bomb: Clandestine code triggered by a certain set of conditions, such as a particular date or a combination of inputs

Mail bombing: Overloading an e-mail system by sending large volumes of messages (also known as e-mail flooding)

Masquerading: Posing as an authorized entity

Network scanning: Using standard network protocols to determine topology and service access points of a target network

Packet sniffing: Copying data in transit on a network link, usually with a network transceiver in “promiscuous mode”

Password cracking: Trying words from a dictionary to ascertain a user password

Ping flooding: Sending a large number of Internet Control Message Protocol (ICMP) “echo” requests to a target system, causing it to divert significant resources to handling them

Replay attack: An attack in which network transmissions, usually authentication sequences such as user login

information, are recorded (see packet sniffing) and later re-sent by a masquerader

Script kiddies: Inexperienced hackers who use prepackaged software to conduct attacks against well-known vulnerabilities

Security audit tools: Software tools that probe systems to discover vulnerabilities so that attackers can quickly identify easy targets (also used as a defense)

Shell escapes: User input, usually to a Web-based forms processor supported by a Common Gateway Interface (CGI) scripting utility, that contains OS commands to be executed unintentionally by a command interpreter

Shoulder surfing: Acquiring data by observing user interaction with computer I/O devices, such as monitors or touchscreens (often accomplished using magnification devices from a distance)

Smurfing: Combination of IP spoofing and ping flooding in which ICMP echo requests and the target subnet address are sent to a group of unsuspecting accomplice systems, which then generate replies to broadcast addresses on the target subnetwork

Social engineering: Using human relationships and interactions to obtain unauthorized access or confidential information

SYN flooding: Beginning Transmission Control Protocol (TCP) sessions with a target system by sending initial synchronization requests but not acknowledging responses, causing the number of open connections on the target system to increase and consume resources

Traffic analysis: Observation of network traffic patterns to deduce confidential information, such as communication habits and frequency (also used as a defense)

Trapdoor: Undocumented program behavior triggered by a secret input sequence to give a perpetrator special privileges

Trojan horse: A software program that is advertised to fulfill a useful function but is actually malicious

van Eck attack: The use of sophisticated reception equipment to capture and decode electromagnetic signals from computer output devices at a distance

Virus: Code fragment inserted into a legitimate program (a process called infection) to steal processor cycles during which new programs are found and infected

War dialing: Automated dialing of every telephone number on a common exchange for the purpose of finding numbers that are connected to computer systems

Worm: A self-replicating program or virus that uses network connections to propagate to new systems

Vulnerabilities that attackers prey upon

Although attackers continue to create new methods for violating computer system security, the vulnerabilities they exploit remain the same. These vulnerabilities can be divided into five types (see “Common Attacks” for specific definitions of attack terms):

» **Implicit trust.** The unquestioning, unchecked acceptance of a person or agent. Attacks that exploit this vulnerability include: compromised system utilities, e-mail forgery, IP spoofing, keystroke monitoring, logic bomb, masquerading, shoulder surfing, social engineering, Trojan horse, trapdoor

COMMON DEFENSES

Anonymity: Removal of any association between a communication source identity and the message it sends

Badges and cards: Authentication schemes based on physical objects within a person’s possession

Biometrics: Authentication schemes based on a physical characteristic of a person’s body

Call-back: Outbound telephone connection from a system to a user’s preregistered telephone number after a request from a previous incoming call

Encryption: The use of algorithms and text or numeric keys to make data unreadable except for those who know the encoding algorithms and keys

Filtering: Selectively blocking communication according to certain criteria

Firewall: A point of controlled communication between a trusted and distrusted network; employs a combination of packet filtering, traffic analysis, and proxy translation

Honeytrap: A computer system set up for the express purpose of attracting and studying computer hackers

Integrity check: Data inspection to detect tampering

Intrusion detection: System monitoring to identify unauthorized entry

Misuse detection: System monitoring to identify misuse of resources by authorized individuals

Packet stuffing: Generating “filler” network transmissions to obfuscate traffic patterns

Password: A shared textual secret

Password checker: An algorithm applied to candidate passwords to determine their “crackability”

Patching: Applying a differential modification to software to repair or enhance its functionality

Peer review: Systematic inspection of a colleague’s work to provide a system of checks and balances

Pinhole: Configuration of a network router or firewall to pass IP traffic only on a single, often unadvertised port

Process review: Periodic evaluation of processes involving human and computer interaction to ensure continued congruence

Public key cryptography: An encryption system that provides authentication and privacy through the use of public and private keys

Reminders: User-directed messages that reinforce security concepts and are triggered by user interaction with the system when the concepts are applicable

Sandbox: An isolated system in which administrators can safely test new software

Security audit tools: Software tools that probe a system to discover vulnerabilities so that administrators can rectify them (also used as an attack)

Shared secret: Information known only to those wishing to communicate; used to establish authenticity

Shielding: Constructing a physical barrier to dampen electromagnetic radiation signals within a computing environment so that attackers cannot detect or scramble the signals

Signature: A check value, called a message digest, computed from the message content using a private key

Steganography: A method of hiding a secret message within a larger, publicly viewable message so that only those who know where to look can read the message

Tip of the day: A daily automatic message sent to a user base to provide incremental training

Traffic analysis: Observation of network transmissions to detect abnormal usage patterns that indicate intrusion or misuse (also used as an attack)

Training: Teaching awareness and proficiency in security objectives to a user base

Trash disposal: Discarding used memory, such as paper documents or magnetic tapes and disks, in such a way that the contents are erased or unreadable

Upgrading: Replacing a software package with a revised version that introduces fixes and new functionality

Virus detection: System monitoring to identify the presence of (and attempts to introduce) viral infections

Watermark: A unique, digital pattern encoded in a document for the purpose of establishing authenticity or tracking ownership; usually only detectable by special means (see also steganography)

- ▶▶ **Configuration error.** An error in configuration or a failure to replace a default configuration with a more secure one. Attacks include: backdoor, bacteria, e-mail relay, IP spoofing, network, scanning, ping flooding, shell escapes, smurfing, war dialing
- ▶▶ **Public information.** Leveraging well-known or easily obtainable information to expose weaknesses or to facilitate an attack. Attacks include: DNS hijack, packet sniffing, security audit tools, traffic analysis, van Eck attack, worm
- ▶▶ **Weak design.** A process or system that was not designed with security as a goal. Attacks include: buffer overrun, DNS hijack, IP spoofing, mail bombing, masquerading, network scanning, ping flooding, replay attack, shell escape, smurfing, SYN flooding, virus, worm
- ▶▶ **Carelessness.** Failure to observe procedures and regimens that would foster a secure environment, such as staying current with software patches or choosing good passwords. Attacks include: backdoor, buffer overrun, password cracking, shoulder surfing, war dialing, virus

Defending a system against security attacks

A defense is a countermeasure for dealing with security attacks. Administrators can employ five types of defenses (see “Common Defenses” for specific definitions of defense terms):

- ▶▶ **Obfuscation.** Confusing the attacker by obscuring publicly available information that exposes vulnerability. Examples include: anonymity, encryption, packet stuffing, public key cryptography, shielding, steganography, trash disposal
- ▶▶ **Authentication and authorization.** Ensuring that a person or system claiming an identity is the real owner of the identity, and granting access on a “must have” basis. Examples include: badges and cards, biometrics, password, shared secret, signature, watermark
- ▶▶ **Monitoring and auditing.** Observing system vulnerabilities, either in real time or through audit tools, to detect attacks. Examples include: filtering, firewall, integrity

check, intrusion detection, misuse detection, password checker, peer review, process review, security audit tools, virus detection

- ▶▶ **Currency.** Consistently using tested software updates and periodically reviewing human processes and procedures. Examples include: patching, process review, upgrading
- ▶▶ **Education and enforcement.** Effectively equipping system designers and users with knowledge of security risks, and then enforcing application of this knowledge. Examples include: reminders, tip of the day, training

Moving forward

The key to preventing security attacks from diminishing system performance is knowledge. IT administrators can develop their security strategies by studying historical and contemporary attacks, appropriate defenses, and the evolving trends in the computer security industry. Online resources such as the CERT Coordination Center at Carnegie Mellon University also provide useful information about current security threats and remedies. 🌐

J. Craig Lowery, Ph.D. (*craig_lowery@dell.com*) is a senior engineer in the Application/Software Development Group of the Dell Enterprise Systems Group, where he currently leads the Dell PowerEdge Cache Server engineering team. Craig received an M.S. and a Ph.D. in Computer Science from Vanderbilt University, and a B.S. in Computing Science and Mathematics from Mississippi College. He is an established radio commentator on technology and his primary areas of interest include networking, programming languages, and operating systems.

FOR MORE INFORMATION

CERT Coordination Center at Carnegie Mellon University:
<http://www.cert.org>