

**FUNDAMENTALS OF
COMPUTER FRAUD**

(No. 99-5403)

III. THE COMPUTER AS A TOOL FOR FRAUD

Common Categories of Computer Fraud

All stages of computer operations are susceptible to criminal activity, either as the target of the crime, the instrument of the crime or both. Input operations, data processing, output operations, and communications have all been utilized for illicit purposes. The more common categories of computer-related crime are discussed here.

Fraud by Computer Manipulation

Intangible assets that are represented in data format, such as money-on-deposit or hours of work, are the most common targets of computer-related fraud. Modern business is quickly replacing cash with deposits transacted on computer systems, creating an enormous potential for computer abuse. The organized criminal community has frequently targeted credit card information, as well as personal and financial information about clients. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative. Assets represented in data format often have a considerably higher value than traditionally targeted economic assets, resulting in potentially greater economic loss. In addition, improved remote access to databases allows the criminal the opportunity to commit various types of fraud without ever physically entering the premises of the victim.

Input Manipulation

Computer fraud by input manipulation is the most common computer crime, as it is easily perpetrated and difficult to detect. Often referred to as “data diddling,” it does not require any sophisticated computer knowledge and can be committed by anyone having access to normal data processing functions at the input stage. Diddling requires a relatively low-level of computer expertise as it generally involves the deliberate entry of false information, a simple task.

Program Manipulation

Program manipulation, which is very difficult to discover and is frequently not recognized, requires the perpetrator to have computer-specific knowledge. This involves changing existing programs in the computer system or inserting new programs or routines. The Trojan horse is an example of a common method of program manipulation used by persons with specialized knowledge of computer programming.

Output Manipulation

Output manipulation is effected by targeting the output of the computer system. The obvious example is cash dispenser fraud, achieved by falsifying instructions to the computer in the input stage. Traditionally, such fraud involved the use of stolen bankcards. However, specialized computer

hardware and software is now being widely used to encode falsified electronic information on the magnetic strips of bankcards and credit cards.

One type of computer manipulation fraud takes advantage of the automatic repetitions of computer processes. Such manipulation is characteristic of the specialized “salami technique,” whereby nearly unnoticeable, “thin slices” of financial transactions are repeatedly removed and transferred to another account.

Computer Forgery and Desktop Counterfeiting

When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery. A new generation of fraudulent alteration or counterfeiting emerged when computerized color laser copiers became available. These copiers are capable of high-resolution copying, modification of documents, and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

These schemes take very little computer knowledge to perpetrate. Counterfeit checks, invoices and stationery can be produced using scanners, color printers and graphics software. Such forgeries are difficult to detect for the untrained eye. It is relatively easy to scan a logo into a computer system and go from there.

EXAMPLE

A company in Dallas, Texas, provided on-site technical support for one of the major personal computer manufacturers. The company took the checks they received from the computer manufacturers in payment of services and created exact duplicates by using off-the-shelf scanners, graphics software, and printers.

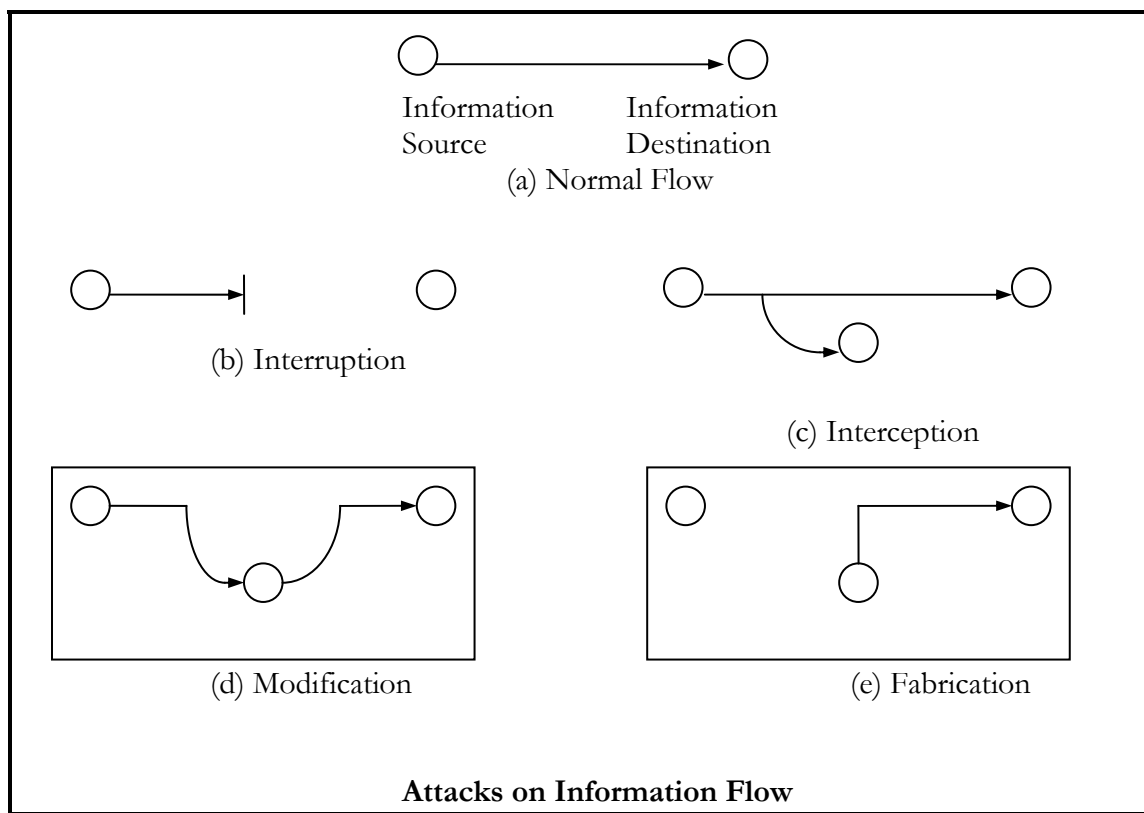
If the double payments were caught, the bank would check their microfiche copies of the two checks, which appeared to be identical, and in many cases assumed that a clerical error had occurred. Several of the banks wrote off the loss as their mistake as a gesture of maintaining good customer relations with their depositors and thus helped the fraudsters continue their scheme for some time. However, the fraudsters were eventually caught and a forensic examination of their computer found scanned images of several counterfeit checks that the suspects thought had been erased from the computer.

Technical Attacks on Computer Security

Categories of Network Security Attacks

Attacks on the security of a computer system or network can be best characterized by viewing the function of the computer system as providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user. When a system is attacked, the normal flow of information is somehow corrupted.

This normal flow of information is depicted in the following figure. The remaining parts of the figure show the four general categories of attack: interceptions, interruptions, modifications, and fabrications.



Interception

Interception occurs when an unauthorized party gains access to an asset. This is an attack on the confidentiality of information assets. Examples can include wiretapping, packet sniffing and key logging to capture data from a computer system or network, and the illicit copying of files or programs.

Interruption

Interruption occurs when an asset of the system is destroyed or becomes unavailable or unusable. This is an attack on the availability of information. Examples include destruction of a piece of hardware,

such as a hard disk; the cutting of a communication line; or the disabling of the file management system. In addition, distributed denial of service attacks (DDoS) also fall into this category as multiple systems are used to temporarily disable a system or network asset.

Modification

A modification attack takes place when an unauthorized party not only gains access to an information asset but also tampers with that asset. This is an attack on the integrity of information. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.

Fabrication

In a fabrication scheme, an unauthorized party inserts counterfeit objects into the system. This is an attack on the authenticity of information. Examples include the insertion of spurious messages in a network or the addition of records to a file.

In addition to the classification discussed above, all network security attacks may be further categorized by whether they are passive or active.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of attacks are involved here: release of message contents and traffic analysis.

RELEASE OF MESSAGE CONTENTS

The release of message contents is easily understood. An electronic mail message, a telephone conversation, or a transferred file may contain sensitive or confidential information. The attacker intercepts the message in order to learn the contents of the communication. This can be accomplished, for example, by wiretapping or packet sniffing¹.

TRAFFIC ANALYSIS

The second passive attack—traffic analysis—is more subtle. Suppose that the contents of messages or other information traffic have been encrypted so that attackers, even if they capture the messages, will not be able to extract the information from the message. Even if an organization has encryption protection in place, an attacker might still be able to observe the pattern of these messages. The attacker could determine the location and identity of communicating hosts and could observe the frequency and

¹ The interception of network traffic to decode and analyze its content.

length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect since they do not involve any alteration of the data. Since detection is not a realistic goal, information security professionals should focus on preventing passive attacks.

Active Attacks

The second major category of attack is active attacks. Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, since to do so would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

MASQUERADE

A masquerade takes place when one entity pretends to be a different entity. For example, a user with low-level privileges may try to impersonate an individual that has a higher level of privileges in order to get access to restricted files. Spoofing and password cracking are common examples of a masquerade attack and are discussed in more detail below.

REPLAY

Replay involves the passive capture of information and its subsequent retransmission to produce an unauthorized effect.

MODIFICATION OF MESSAGES

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning “Allow John Smith to read the confidential file *accounts.doc*” is modified to mean “Allow Fred Brown to read the confidential file *accounts.doc*.”

DENIAL OF SERVICE

The denial of service attack prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security manager). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages to degrade performance.

Common Methods of Attack

Attacks are deliberate attempts to interfere with the intended use of a system by means of exploiting some of the known vulnerabilities inherent in the modern computer system. The following sections discuss some common methods of attacks on computer systems.

Social Engineering

One of the most common ways to gain unauthorized entry into a computer system is to obtain the password of a legitimate user. This is most frequently accomplished through social engineering. In a social engineering scheme, the perpetrator tricks a user into revealing his or her password and userID. In a typical scenario, a hacker calls the help desk of a target company. The hacker pretends to be a new employee on his first day of work. The hacker tells the help desk employee that he cannot log-on to his computer because no one has given him a password and userID. The help desk employee provides a temporary password that enables the hacker to enter the system. Social engineering is thought to play at least some part in most computer system penetrations.

Dumpster Diving

Another non-technical method outsiders use to obtain passwords is dumpster diving. In this rather unglamorous technique, the hacker digs through a target's trash, looking for correspondence, discarded computer media, telephone or e-mail directories or other information that will help grant the spy access to the target's network.

Shoulder Surfing

Still another non-technical method is known as shoulder surfing, in which the spy simply looks over someone's shoulder as they log-on to the system. This may enable a spy to learn the user's password, userID, and other useful information.

Browsing

Browsing is one of the simplest network attacks. It involves the search of large quantities of available data in an attempt to identify sensitive information. Browsing, for example, may involve searching physical memory for the system password table, or scanning files in disk storage for confidential information. The best way to defend against browsing attacks is to establish a strong access control system.

Unsecured Offices

Leaving passwords in obvious locations is another easy way for an unauthorized person to obtain log-on information. Many office workers tend to leave their password reminder lists within arm's reach of their computer. This can be an easy target for after-hours personnel, such as contract cleaning crews, who have unlimited access to work spaces.

Password Cracking

Password cracking is an automated process by which an attacker attempts to guess the most likely passwords of a system user. A password cracker will typically try to exploit users who employ personal, easy-to-figure-out passwords such as their name, their children's or spouse's name, their nickname, the name of a pet, etc. As was discussed earlier, this information is frequently obtained by an attacker through a fictitious survey, a fake prize, or some other social engineering scheme. If the standard attack does not work, the most common methods of cracking a password are dictionary attacks and brute force attacks.

DICTIONARY ATTACKS

In this form of attack, the intruder utilizes a program that will try every word in the dictionary as a password. A dictionary attack program can run approximately 1,000 words per second or more. The dictionary can be expanded to include things like common first names, movie titles and sports terms, as well as foreign languages. There are even lists of common passwords that can be incorporated into the dictionary. Every word is also arranged in several ways, varying upper and lower-case letters, reversing the spelling, substituting numerals 0, 1, 2 and 5 for the letters O, I, Z and S. Obviously, one of the best ways to defeat a dictionary attack is to use randomly generated, nonsensical passwords instead of actual words or names.

BRUTE FORCE ATTACKS

Brute force attacks are similar to dictionary attacks, but here the attacker tries every possible combination of characters, not just every word in the dictionary. (For example, accxj29 is not a word, but could still be somebody's password). Obviously, it can take much longer for an automated system to run through every possible combination of characters.

The principal defense against a brute force attack is to increase the cost of the attack by increasing the number of possibilities to be exhausted. While a four-letter password can be cracked in a matter of minutes, an eight-character password that is case sensitive and includes numbers and punctuation marks among its possible characters, could take months to crack using a standard brute force program.

Spoofing

Spoofing is an attack in which one user pretends to be a different user that has more privileges. A spoof is generally used to fool a user or a system into volunteering information. Suppose, for example, that a hacker wants to get access to Process A. The hacker is not authorized to utilize Process A, but Joe, a system user, is authorized to use it. The hacker will essentially trick Process A into thinking that the hacker is really Joe. In the absence of any other controls, Process A may be spoofed into granting the hacker access to the data and privileges that were meant for Joe.

LOG-IN SPOOF

One way to spoof is to set up a program between the user terminal and the main system. The program duplicates the action of an existing command or program, but it is run without the user's knowledge. In a log-in spoof, a program is planted on the terminal of a targeted user. This program simulates the log-in sequence that normally appears on the terminal when the user logs-in to the main system. In other words, when the user turns on their computer, it looks like the normal log-in prompt appears, but what they are actually seeing is the duplicate program inserted by the attacker.

Believing that they are communicating with the legitimate system, the user enters their ID and password. Now the user's log-in information has been compromised. The spoofing system tells the user that the password was entered incorrectly or that the legitimate system is experiencing a problem. The attacker promptly plays the captured ID and password back to the target system, which accepts the attacker as a legitimate user.

IP SPOOFING

IP spoofing is a method of attack in which a hacker convinces the system under attack that he is someone else by forging the IP address of another user. The intruder is then able to send commands to the server under the disguised IP source addresses, making it difficult or impossible to trace the actual source of the messages.

Sniffing

Password sniffers are computer programs that monitor traffic on areas of a network, searching packets of data as they pass through the network. When a message is transmitted across the Internet, for example, it flows through many computer nodes as it makes its way to its final destination. Sniffing programs can be embedded in nodes so that they read all the packets of information that pass through those nodes, looking for passwords that will help the hacker gain access to a restricted system.

When a user logs onto an Internet service provider, he usually has to type in a user name and a password. Most sniffing programs collect the first portion (128 bytes or more) of each network connection being monitored. (This is where the username and password are most likely to be found.) Items like usernames and passwords are then sniffed out of the collected information to be used by the attacker.

Pinging and Flooding

Pinging and flooding are denial of service attacks in which the attacker overloads the communication ports of the victim. This is analogous to a telephone system that is overloaded when too many people call the same number at the same time. The result of these schemes is that the victim is unable to provide service to its legitimate customers because its system has been overburdened.