ATTACKS ON CRYPTOSYSTEMS

Man-in-the-Middle Attack

A man-in-the-middle attack, as discussed in Chapter 2, is designed to intercept the transmission of a public key or even to insert a known key structure in place of the requested public key. Thus, attackers attempt to place themselves between the sender and receiver, and once they've intercepted the request for key exchanges, they send each participant a valid public key, which is known only to them. From the perspective of the victims of such attacks, their encrypted communication appears to be occurring normally, but in fact the attacker is receiving eac
encrypted message and decoding it (with the key given to the sending party), and then encrypting signatures can prevent the traditional man-in-the-middle attack, as the attacker cannot duplicate

Dictionary Attacks

In a **dictionary attack**, the attacker encrypts every word in a dictionary using the same
cryptosystem as used by the target. The attacker does this in an attempt to locate a match between the target ciphertext and the list of encrypted words from the same cryptosystem. Dictionary attacks can be successful when the ciphertext consists of relatively

few characters, as for example files which contain encrypted usernames and passwords. If an attacker acquires a system password file, the individual can run hundreds of thousands of potential passwords from the dictionary he or she has prepared against the stolen list. Most computer systems use a well-known one-way hash function to store passwords in such files, but this can almost always allow the attacker to find at least a few matches in any stolen password file. After a match is located, the attacker has essentially identified a potential valid password for the system under attack.

Timing Attacks

In a **timing attack**, the attacker eavesdrops during the victim's session and uses statisticalanalysis of the user's typing patterns and inter-keystroke timings to discern sensitive session information. While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem in use. It may also eliminate' some algorithms as possible candidates, thus narrowing the attacker's search. In this narrower field of options, the attacker can increase the odds of eventual success. Once the attacker has successfully broken an encryption, he or she may launch a **replay attack**, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.

Defending From Attacks

Encryption is a very useful tool in protecting the confidentiality of information that is in storage and/or transmission. However, it is just that-another tool in the information security administrator's arsenal of weapons against threats to information security. Frequently, unenlightened individuals describe information security exclusively in terms of encryption (and possibly firewalls and antivirus software). But encryption is simply the process of hiding the true meaning of information. Over the millennia, mankind has developed dramatically more sophisticated means of hiding information from those who should not see it. No matter how sophisticated encryption and cryptosystems have become, however, they have retained the same flaw that the first systems contained thousands of years ago: If you discover the key, that is, the method used.