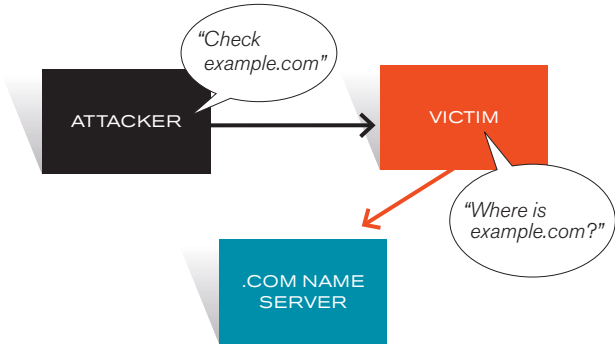


A CACHE-POISONING ATTACK

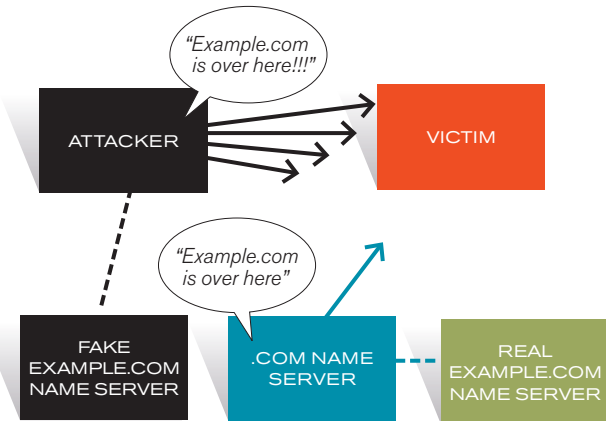
Cache poisoning causes a requesting server to store false information about the numerical address associated with a website. A basic version of the attack—without some of the more sophisticated techniques Kaminsky employs—is outlined below.



1. To begin, the attacker lures the victim's server into contacting a domain the attacker controls. The attacker could, say, claim to have forgotten a password, prompting the victim to respond by e-mail.



2. The victim performs a DNS lookup to find out where to send the e-mail. But the attacker's name server refers the victim to another server, such as that of example.com. Since the attacker knows that the victim will now start a DNS lookup for that server, he or she has an opportunity to attempt to poison its cache.



3. The attacker tries to supply a false response before the legitimate server can supply the real one. If the attacker guesses the right ID number, the victim accepts the false reply, which poisons the cache.