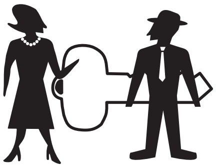

PART III

DISTRIBUTION OF PUBLIC KEYS

Public key cryptography changed 3,000 years of key exchange. For thousands of years, Alice and Bob had to somehow exchange a secret key without anyone else's seeing it. Furthermore, the shared secret key had to remain secret forever. Public key cryptography changed all that, allowing Alice (and Bob) to exchange public keys openly. Public keys don't need to be secret. In fact, some Internet companies want as many people as possible to know their public keys.

Even though public keys can be openly distributed, recipients need assurances that they are receiving the genuine public key.

But as we've seen, even though Alice can openly distribute her public key to Bob, they need assurances that BlackHat can't substitute his public key for Alice's public key. For example, in Figure PIII-1, after BlackHat successfully mounts a man-in-the-middle attack (see Chapter 22) between Alice and Casey, he can read Casey's confidential messages to Alice and masquerade as Alice to Casey. As a result, delivery of authentic public keys is still a problem.

Let's use a real Internet e-commerce example. Amazon.com wants you to feel secure when you communicate with it. The company sends you its public key so that you can send it confidential messages (encrypt with its public key). You also use Amazon's public key to verify the company's signed (private key en-

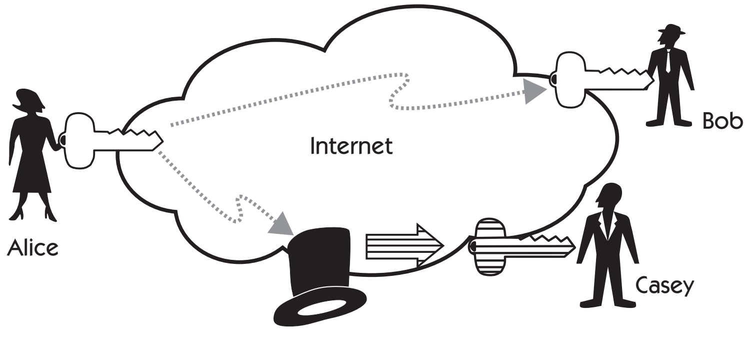

Figure PIII-1 Alice openly distributes her public key to Bob and Casey. But BlackHat intercepts the key on the way to Casey and substitutes his public key for Alice's public key.

crypted) messages (to make sure they're really from Amazon and not from one of its competitors). You must trust that you have Amazon's authentic public key. How does Amazon get you its public key? The popular current answer is to use digital certificates. Digital certificates are used in real-world systems such as Secure Socket Layer (SSL), secure e-mail (S/MIME and PGP), virtual private networks (VPNs) and Internet Protocol Security (IPsec), to name a few.

Chapter 16 examines how digital certificates protect public keys and explains why BlackHat has a much more difficult job corrupting public keys when they are wrapped in and delivered with digital certificates, as shown in Figure PIII-2.

After explaining how digital certificates protect public keys, we discuss two popular standards—X.509 and PGP—in Chapters 17 and 18, respectively.

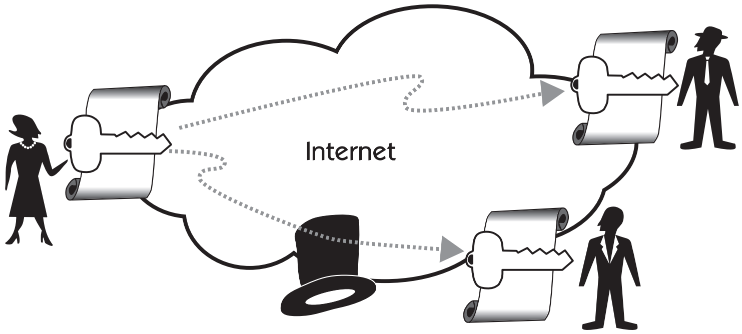

Figure PIII-2 Alice openly distributes her digital certificate. BlackHat can't easily substitute his public key for Alice's public key.