PART IV
REAL-WORLD SYSTEMS

Now that we've presented all the ingredients (secret keys, public/private keys, hash functions, and digital certificates) for cryptographic systems, let's see how those pieces operate collectively in the real world. In the next five chapters we show how secure e-mail (S/MIME, PGP), Secure Socket Layer (SSL), and Internet Protocol Security (IPsec) provide security. We also describe a few famous attacks and discuss how to protect your keys.

These real-world systems implement some or all of the cryptographic assurances we've been discussing since Chapter 1: authentication, confidentiality, integrity, and nonrepudiation. In addition, because all three systems encrypt the majority of their data with a secret key, each includes (secret) key agreement or key exchange.[1]

Although the three systems don't implement the assurances and key exchange in the same order, they all follow roughly the path shown in Figure PIV-1. Secure e-mail users can demand all the protections shown here, and, with the exception of nonrepudiation, so can SSL and IPsec users.

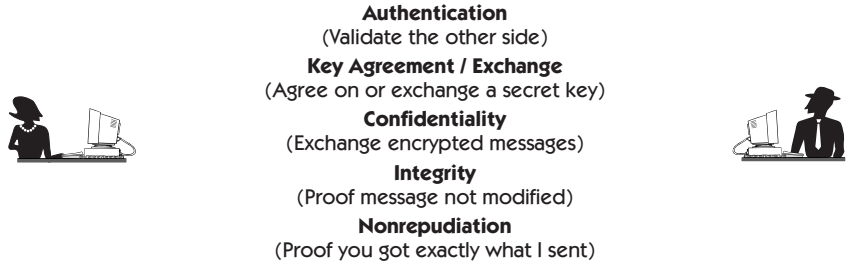

Figure PIV-1 General flow and attributes of cryptographic systems, secure e-mail, SSL, and IPsec.

1. In this text, *key exchange* means that Alice encrypts a secret key with Bob's public key and sends it to Bob. *Key agreement* means that Alice and Bob independently compute the identical secret key using Diffie-Hellman. At times we also use *key exchange* more broadly to apply to both situations.

Mel pt IV 203 3/15/01, 11:02 AM

E-mail Cryptographic Parameters

Alice's e-mail messages to Bob usually go to Bob's e-mail server and usually are not sent directly to Bob's computer. Bob can retrieve Alice's e-mail after Alice sends it, whether or not Alice is still connected to the Internet.

An e-mail sender unilaterally picks cryptographic assurances and parameters.

Alice unilaterally chooses her cryptographic protections and parameters. So an e-mail receiver doesn't negotiate cryptographic assurances or parameters with an e-mail sender; the receiver takes it or leaves it. For example, if Alice encrypts e-mail with Triple DES, Bob's computer must be able to decrypt using Triple DES. This shouldn't be a problem if both e-mail users are using the same cryptographic program—for example, PGP.[2]

Negotiation of SSL and IPsec Cryptographic Parameters

SSL and IPsec users negotiate cryptographic assurances and parameters.

Unlike secure e-mail, SSL and IPsec assume that Alice's and Bob's computers are connected to each other, and they allow Alice and Bob to negotiate which cryptographic assurances and parameters they want to use (see Figure PIV-1).

SSL assumes that a client and a server relationship exists between the two parties: A customer (for example, Bob) wishes secure exchanges with some merchant (for example, AliceDotComStocks). IPsec, on the other hand, treats each end of the connection in the same way. Both SSL and IPsec first exchange plaintext in which Bob sends a greeting to Alice and offers a variety of potential suites of cryptographic parameters from which Alice should choose (see Figure PIV-2).

Overview of SSL and IPsec

SSL and IPsec can be roughly categorized as two-part systems, as shown in Table PIV-1. In part 1, both SSL and IPsec exchange plaintext messages, authenticate each other, and agree on secret keys. In part 2 they use their agreed-

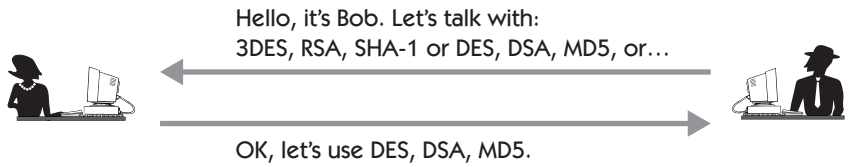

Figure PIV-2 A first SSL or IPsec message.

2. But some older versions of a program (such as PGP) may be incompatible with newer versions of the same program.

on secret keys to encrypt (decrypt) confidential messages with integrity. Both SSL and IPsec offer assurances in many different ways; for example, depending on the situation, secret key exchange may be completed before authentication.

Table PIV-1 General overview of IPsec and SSL as two-part systems. They first exchange plaintext messages, authenticate each other, and agree on secret keys; then they use the secret keys to exchange confidential messages with integrity.

	Part 1
Hello There	Bob initiates an Internet connection with Alice
Authentication	Bob challenges Alice: prove you have private key
	…and then Alice challenges Bob
Key exchange	Exchange secret key
	Part 2
Confidentiality	Encryption using secret key cryptography
Integrity	Detect whether confidential messages altered in transit

Note that neither SSL nor IPsec offers nonrepudiation.

User Initiation of Cryptographic E-mail, SSL, and IPsec

Cryptographic e-mail applications and SSL require that the user explicitly invoke cryptographic protections. For example, as you'll see, an e-mail user must select the option of encrypting his or her e-mail. Similarly, a user must invoke SSL.

In contrast, IPsec provides its cryptographic protections by default and does not require invocation by the user. In fact, IPsec is meant to be transparent to the user, who may not be aware IPsec is even installed on the computer.