~/.ssh/known\_hosts

How do you want to update your key cache? In some environments, users must manually verify host keys and then manually add them to the key cache. In other environments, it's acceptable to automatically add new keys to the cache. Most commonly, users want ssh to ask them what to do. The StrictHostKeyChecking *ssh\_config* option tells ssh how to treat new host keys.

If you want to only add host keys to *known\_hosts* by hand, set StrictHostKeyChecking to yes. When you connect to a new host, ssh will present the host key and tell you to verify it and add it to known\_hosts yourself. You will not be able to connect until you add the key. Additionally, when a host key has changed, ssh will refuse to complete the connection, instead displaying a warning and telling you to verify the key. This is most useful when the systems administrator regularly updates */etc/ssh/known\_hosts* (see Chapter 13).

StrictHostKeyChecking yes

At the other extreme, you can have ssh automatically add unknown host keys to *known\_hosts*. By having your client accept all host keys, you have no opportunity to verify the host key. Accepting unverified host keys is dangerous, as discussed in Chapter 4. To blindly accept all host keys, set StrictHostKeyChecking to no. But don't do it.

By default, ssh displays unknown host keys and asks the user what it should do. You can either choose to accept the host key and have ssh add it to *known\_hosts*, or reject the host key. StrictHostKeyChecking defaults to*ask*.

Choose the option that best suits your environment. Your home computer probably has different needs than a secure system run by the NSA or a criminal cartel.