**Preventing SSH Security Problems**  
SSH is intended to solve security problems rather than create them. Indeed, on the whole,  
using SSH is superior to using Telnet for remote logins, and SSH can also take over FTPlike functions and tunnel other protocols. Thus, SSH is a big security plus compared to  
using less-secure tools.  
Like all servers, though, SSH can be a security liability if it’s run unnecessarily or  
inappropriately. Ideally, you should configure SSH to accept *only* protocol level 2 connections and to refuse direct root logins. If X forwarding is unnecessary, you should disable  
this feature. If possible, use TCP wrappers or a firewall to limit the machines that can  
contact an SSH server. As with all servers, you should keep SSH up to date; there’s always  
the possibility of a bug causing problems.  
You should consider whether you really need a remote text-mode login server. Such a  
server can be a great convenience—often enough to justify the modest risk involved. For  
extremely high-security systems, though, using the computer exclusively from the console  
may be an appropriate approach to security.  
One unusual security issue with SSH is its keys. As noted earlier, the private-key files are  
extremely sensitive and should be protected from prying eyes. Remember to protect the backups of these files as well. Protect system backup files as securely as you would the originals.